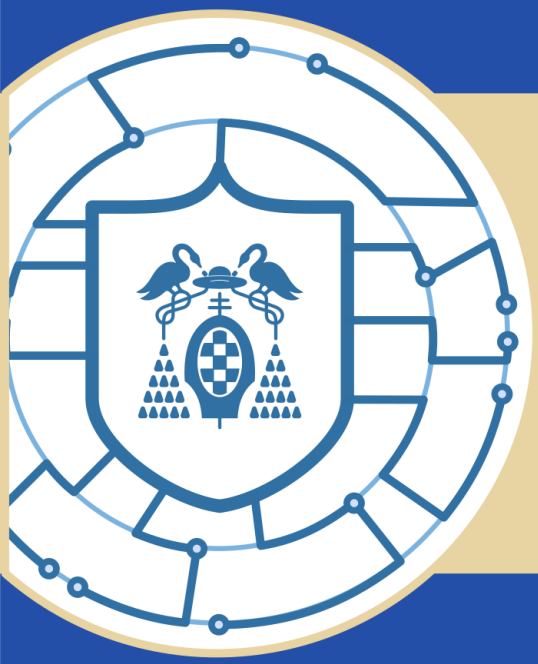
MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD



Comparativa de herramientas y utilidades para la adquisición de datos de la memoria RAM

TRABAJO FIN DE MÁSTER

Autor: Alejandro Fernández Maceira

Director: José Javier Martínez Herráiz

Universidad de Alcalá

2021

Escuela de Posgrado

Índice

Índice de figuras

Índice de tablas

1. Introducción

El análisis forense digital está más presente que nunca. Cada vez se dan más casos de ataques de virus informáticos, sobre todo de ransomware, lo que conlleva una investigación asociada para averiguar la máxima información posible acerca del ataque. El primer paso en cualquier procedimiento de investigación forense digital es la identificación de los activos informáticos que se deben revisar para obtener información. A partir de esta identificación, comienza la fase de adquisición de evidencias. Esta adquisición debe realizarse siguiendo un procedimiento que garantice y asegure la cadena de custodia de la información, de forma que se mantenga su integridad y se pueda identificar al autor de la adquisición en todo momento.

Una de las primeras ubicaciones de información que se debe revisar es la información volátil, la que no se mantiene cuando se apaga el equipo informático. Adquirir esta información debe ser la principal prioridad cuando se trabaja con un equipo informático encendido, y dentro de esta información volátil destaca la memoria RAM.

En el caso de esta memoria, cuando se desconecta la electricidad del equipo, el contenido es eliminado de forma permanente, y se vuelve a escribir al iniciar de nuevo el equipo, pero con otra información. En este proceso, si se está analizando el equipo tras un ataque de malware, la información que podría ayudar a dar con él se perderá para siempre, pudiendo dificultar o imposibilitar el futuro procedimiento de análisis forense. Otra consideración a tener en cuenta es que cuando se trabaja en respuesta ante incidentes, se ha de ser especialmente cuidadoso con la memoria RAM. Cualquier modificación que sobrescriba el contenido de la memoria, como crear nuevos archivos, puede hacer que se pierda parte de la información contenida en la misma.

Es por esta razón por la que la adquisición, clonado o exportación de la memoria RAM es una de las tareas más importantes a realizar en un equipo, con el añadido de que se debe conseguir de forma que no se modifique la memoria en el proceso, o de lo contrario la investigación podría ser inútil. Las herramientas que se utilicen deben ser rápidas, confiables, seguras y que mantengan la integridad de los datos obtenidos sin modificar en la medida de lo posible la memoria original.

2. Objetivo

El objetivo principal de este trabajo es realizar una comparativa práctica y teórica sobre varias herramientas de adquisición de datos de la memoria RAM, analizando sus características en profundidad y comparándolas entre sí. Se realizarán pruebas de velocidad de captura de datos con cada herramienta tanto en disco duro HDD como en disco duro de estado sólido SSD, de forma que se observará qué herramienta es la más rápida en distintos escenarios. Para una mejor identificación de las mejores herramientas según unos criterios objetivos, se incluirá un apartado de valoración final en el que se indiquen las ventajas, desventajas y una calificación numérica de la herramienta.

Otro objetivo de este trabajo es la identificación las de herramientas más adecuadas para la realización de diversas tareas, como el análisis forense. Para ello, se investigarán las características específicas de cada utilidad en relación al tipo de tarea que corresponda, mostrando las herramientas más adecuadas y recomendables para esa tarea.

Un objetivo secundario de este trabajo es mostrar las distintas opciones de adquisición de memoria RAM en distintos entornos. Se utilizarán los dos sistemas operativos más extendidos en la actualidad, Windows y Linux, y se analizarán los modos de captura de datos de la memoria volátil que utilizan las herramientas para poder obtener esta información y saltar las medidas de seguridad de estos sistemas operativos.

Por último, el trabajo busca acercar el conocimiento de las herramientas de adquisición de memoria RAM a los investigadores forenses y otros usuarios que busquen el modo de extraer esta información de un equipo. Para lograrlo, se incluirá un apartado de experiencia de usuario, en el que se detallará la facilidad de uso de la utilidad, la complejidad de ejecución y de captura y otras características que puedan indicar un uso más sencillo o difícil de la herramienta.

3. Estado del arte

El estudio de la memoria RAM en un análisis forense es uno de los principales métodos de obtención de información en un equipo informático por varias razones, pero principalmente por su carácter volátil. En los últimos años se han realizado numerosos avances en cuanto a formas de trabajar con la memoria RAM. Estos avances se han centrado principalmente en la aparición de nuevos tipos de memoria RAM más rápidos y baratos que los existentes, por lo que las técnicas y procedimientos forenses para volcar y analizar la memoria se han tenido que adaptar a los nuevos tipos disponibles.

3.1. Memoria RAM

La memoria RAM (Random Access Memory) es un tipo de almacenamiento de información en la que se escriben datos de forma aleatoria, reduciendo el tiempo de acceso a la memoria. Es por esto por lo que la velocidad de lectura y escritura es la misma sin importar la ubicación física de la información [1]. Esta memoria está organizada en páginas, pero cuando se escribe la información no se sigue un orden concreto, sino que pueden encontrarse datos del mismo archivo en distintas páginas. Dentro de esta memoria se distinguen varios tipos según su fabricación o su tamaño.

3.1.1. Tipos de memoria RAM

Existen dos tipos principales de memoria RAM, dinámica y estática. Por una parte, la memoria dinámica, conocida como DRAM, es la más extendida y la que utilizan la mayoría de ordenadores. Está formada por celdas, y cada una contiene un transistor y un condensador en un circuito integrado, donde se almacena un bit. Los transistores sufren pérdidas de energía con el tiempo, lo que provoca la descarga de los condensadores. Para mantener los condensadores cargados y no perder la información, se suministra carga eléctrica cada pocos milisegundos. Por el contrario, la memoria estática, conocida como SRAM, mantiene la información en la memoria mientras que se suministre energía. Esto la hace más rápida, pero también más cara, por lo que se emplea la memoria DRAM en el uso general.

Dentro del tipo de memoria DRAM, destaca la memoria DRAM síncrona (SDRAM), la cual sincroniza la velocidad de la memoria con la de la CPU, de forma que el controlador SDRAM sabe cuándo va a estar disponible la información solicitada, permitiendo a la CPU realizar más instrucciones sin esperar a la RAM. Actualmente, se emplean las memorias Double Data Rate SDRAM (DDR SDRAM), que son un tipo específico de memoria síncrona que duplica el ancho de banda de la memoria SDRAM funcionando a la misma velocidad. Este incremento se consigue permitiendo la transferencia de información en el flanco de bajada y de subida de una señal de reloj, sin necesidad de aumentar la frecuencia. Las memorias RAM de tipo DDR son las más extendidas y utilizadas en la actualidad, siendo el estándar la versión DDR3 y DDR4.

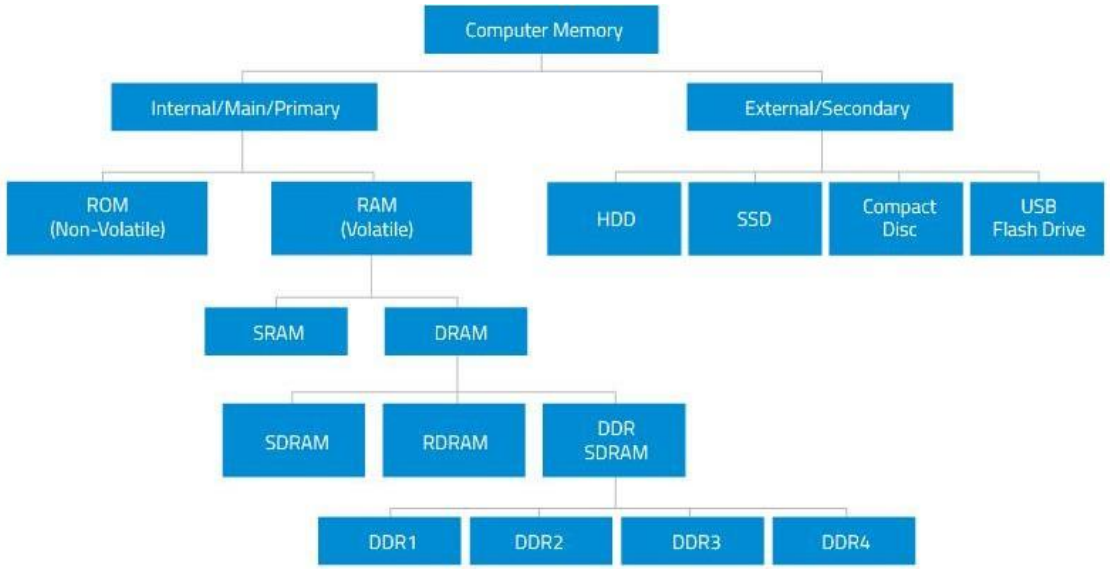


Figura 1. Esquema de los tipos de memoria [2].

Además, dependiendo del tamaño del módulo en el que se instala la memoria RAM, se distinguen dos tipos de módulos, DIMM (Dual In-Line Memory Module) y SO-DIMM (Small-Outline Dual In-Line Memory Module). En general, en los módulos de memoria tipo DIMM, los pines se encuentran a ambos lados del módulo. La diferencia entre DIMM y SO-DIMM se encuentra en el tamaño del módulo, los de tipo DIMM son más grandes y se emplean en equipos de sobremesa y servidores, mientras que los de tipo SO-DIMM son más pequeños y se encuentran en equipos portátiles, tablets o notebooks.

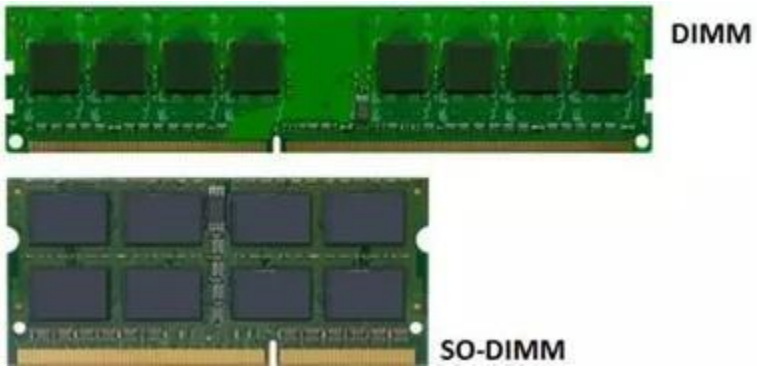


Figura 2. Diferencia entre memoria DIMM y SO-DIMM [3].

Por último, en la siguiente tabla se muestra una comparación de las características de las memorias RAM de tipo DDR3 y las de tipo DDR4.

CARACTERÍSTICA	DDR3	DDR4
VOLTAJE	1,5V en modo por defecto 1,65V en alto rendimiento 1,35V en modo bajo voltaje	1,2V por defecto 1,35V en alto rendimiento 1,05V en modo bajo voltaje
VELOCIDAD	800 MHz, 1066 MHz, 1333 MHz, 1600 MHz, 1866 MHz	800 MHz, 1600 MHz, 2133 MHz

MÓDULOS	DIMM de 240 pines y SO-DIMM de 204 pines	DIMM de 288 pines y SO-DIMM de 260 pines
RELOJ DEL BUS	400-1066 MHz	1066-2133 MHz
TASA INTERNA	100-266 MHz	100-266 MHz
TASA DE TRANSFERENCIA	0,80-2,13 GT/s	2,13-4,26 GT/s
ANCHO DE BANDA	6.40-17.0 GBps	12,80-25,60 GBps

Tabla 1. Comparativa RAM DDR3 y DDR4 [4].

3.1.2. Avances en memoria RAM

Actualmente se comercializan principalmente las memorias RAM de tipo DDR3 y DDR4 para equipos de sobremesa, portátiles y tablets, mientras que la memoria SRAM está reservada para los equipos más importantes, como super servidores. Los avances en cuanto a memoria RAM se centran en expandir las velocidades de las memorias más extendidas, la RAM de tipo DDR.

En el tercer trimestre de 2021 se empezarán a comercializar las primeras memorias RAM de tipo DDR5 de la mano de la empresa TeamGroup. Estas memorias duplicarán la velocidad de transferencia y reducirán el consumo un 10% respecto a las actuales DDR4[5]. Este tipo de estándar está desarrollado por el JEDEC, una empresa internacional especializada en crear estándares para la industria microelectrónica, además de estar acreditada por el Instituto Americano de Estándares (ANSI) [6]. Con el estándar DDR5 desarrollado, cada vez son más los fabricantes de memorias que empiezan a adoptar este modelo de memoria, como Corsair, que asegura poder crear memorias con ancho de banda de 51 Gbps, el doble que en DDR4, y con un tamaño teórico de hasta 128 GB [7]. En los próximos meses se verán más fabricantes anunciando la comercialización de memorias RAM de tipo DDR5, hasta que dentro de pocos años se convierta en el tipo por defecto de memoria.

3.2. Análisis forense

El análisis forense es el proceso de utilizar el conocimiento científico para preservar, recopilar, examinar e informar de la evidencia ante un juez [8]. Este proceso trata de recuperar y analizar las posibles evidencias que existan en todo lo relacionado con la investigación. En el caso del análisis forense digital, las evidencias se encontrarán en equipos como ordenadores de sobremesa, portátiles, tablets o smartphones, pero también en equipos de red o sistemas en la nube. Una vez identificado el equipo a analizar se debe investigar en profundidad para encontrar las posibles pruebas y evidencias que demuestren una hipótesis.

Lo más importante en un análisis forense es seguir un procedimiento bien definido que asegure una correcta validez e integridad de los resultados obtenidos. Es por eso que a lo largo de los años se han ido creando estándares de calidad que regulen el procedimiento del análisis forense desde la adquisición de la información hasta la presentación de las pruebas. Algunas de las normativas más importantes relacionadas con el análisis forense son la ISO 27037, que propone una guía para la identificación, recolección, adquisición y preservación de la evidencia digital [9]; la RFC 3227, que recoge medidas para recopilar y almacenar evidencias de forma segura [10]; y el CFTT (Computer Forensics Tool Testing Program), publicado por el NIST, que proporciona una serie de metodologías de prueba de herramientas software de análisis forense según su funcionalidad [11].

En España también se han creado estándares relacionados con el análisis forense, como la norma UNE 71506:2013 de la Asociación Española de Normalización y Certificación (AENOR). En esta norma se define la metodología y el proceso del análisis forense dentro del ciclo de gestión de las evidencias electrónicas a partir de su adquisición, indicando las fases que se deben seguir para mantener la seguridad en el ciclo de administración de la evidencia digital [12]. Las fases que forman el proceso recogido en la UNE 71506 son las siguientes.

- Preservación de las evidencias originales.
- Adquisición de las evidencias según dispositivo y sistema.
- Documentación del proceso para garantizar la cadena de custodia.
- Análisis de las evidencias obtenidas.
- Presentación de los resultados.

3.2.1. Análisis forense de memoria volátil

En la fase de adquisición de evidencias digitales se sigue un procedimiento definido en el que se prioriza la información volátil sobre la no volátil, por lo que tiene una mayor importancia adquirir antes memorias como la RAM que otras como discos duros. La memoria RAM es un tipo de memoria volátil que es muy importante desde el punto de vista del análisis forense. En casos de respuesta ante incidentes, analizar la memoria volátil puede proporcionar más información sobre el incidente que la memoria no volátil. Detalles como procesos en ejecución, librerías cargadas, usuarios con la sesión iniciada, conexiones de red establecidas o ficheros abiertos están solo disponibles en memoria volátil [13]. Esta información, unida a la obtenida de memoria no volátil, puede proporcionar el contexto necesario para resolver el incidente.

Cuando el equipo de respuesta ante incidentes llega a la escena, se pueden realizar dos acciones principales en cuanto a adquisición de evidencias digitales: desconectar la corriente o interactuar con los equipos. La primera opción es útil en casos en los que se desee analizar la memoria no volátil de discos duros, pues si, por ejemplo, existe un malware que borra información del disco duro, desconectar la energía del equipo evitará que esto suceda, aunque pueda tener consecuencias como corrupción parcial o total del sistema de archivos [14]. La segunda opción, sin embargo, es la única posible en caso de que se necesite investigar la memoria volátil, pues si se desconecta la corriente del equipo se perderá la información contenida en esta memoria para siempre. No obstante, se debe tener en cuenta que realizar tareas de respuesta ante incidentes en el equipo encendido modificará el contenido de la memoria, lo que puede provocar la pérdida de evidencias potenciales que ayuden en la investigación.

En un incidente informático, se debe obtener la información de la memoria RAM de los equipos afectados para después analizarla en un entorno de laboratorio controlado, extrayéndola del equipo afectado sin modificarla en el proceso. Obtener una copia de la memoria RAM se denomina volcado de datos. Un volcado de datos de memoria RAM es una copia bit a bit de la memoria física de un sistema. Cuando se realiza el procedimiento de extracción, se debe tener cuidado de no modificar los datos presentes en la memoria, pues podría perderse información vital para resolver el incidente. Por este motivo, se deben utilizar herramientas de obtención de información de la memoria que mantengan la integridad de los datos obtenidos sin modificar los datos presentes en memoria.

4. Análisis de herramientas de adquisición de memoria RAM

En este apartado se realizará una descripción teórica de cada herramienta, enumerando sus características principales y comparándolas entre las distintas herramientas. Primero, se explicarán las características mínimas necesarias que debe tener una herramienta de adquisición de memoria RAM para extraer la información. Después, se analizarán las herramientas seleccionadas en la comparativa atendiendo a sus características y propiedades relacionadas con el volcado de datos de la memoria. Por último, se realizará una valoración objetiva sobre la mejor herramienta según sus características y funcionalidades, teniendo también en cuenta otras consideraciones como portabilidad y espacio necesario en disco para su uso.

4.1. Características generales de las herramientas

Existen multitud de herramientas de adquisición de memoria RAM, desde suites forenses completas con extracción y análisis de memoria, hasta ligeros ejecutables open source de obtención de memoria que ocupan unos pocos megabytes. Aun así, las funcionalidades principales que se requieren de una herramienta de extracción de memoria RAM deben ser las mismas sin importar su tamaño o licencia de uso. Concretamente, las características más importantes que se van a tener en cuenta en la posterior evaluación comparativa son las siguientes.

- Velocidad de obtención del volcado de datos. La característica principal de cualquier herramienta, con qué velocidad se obtienen los datos de la memoria RAM. Dependiendo de la velocidad de creación del archivo de volcado de datos, la herramienta será mejor candidata para su uso que otra más lenta. Aun así, esta característica no debe ser la única por la que se decida elegir una herramienta sobre otra, pues es posible que extraiga los datos rápidamente, pero consuma muchos recursos del equipo en el proceso, lo que puede ser un factor decisivo cuando se realiza un volcado de datos de la memoria RAM en equipos antiguos y en general menos potentes.
- Impacto en el rendimiento del equipo. Las herramientas que analicen la memoria RAM deben tener el menor impacto en el rendimiento del equipo analizado posible. Obtener el volcado de datos debe ser una tarea que se pueda realizar en equipos antiguos o menos potentes que otros, con hardware más desactualizado y que no tengan tanta capacidad de procesamiento. En resumen, el proceso de volcado debe ser el mismo para todos los equipos sin importar su hardware, software, capacidad de procesamiento, o características técnicas.
- Opciones adicionales de captura. Otra de las características más importantes de una herramienta de captura son las opciones adicionales que presenta para la captura. En estas opciones se tiene en cuenta si la herramienta permite establecer por ejemplo un límite entre zonas de memoria a capturar, o si se pueden incluir archivos e información adicional a la captura para su posterior análisis forense.

No solamente se deben tener en cuenta estas características principales, sino que a la hora de comparar distintas herramientas, puede darse el caso de que estas estén muy igualadas en estos campos, por lo que se hace necesario introducir otras características secundarias a la comparación.

Si bien las funcionalidades secundarias no son las más importantes en una herramienta desde el punto de vista técnico, sí que pueden hacer más atractiva su utilización en distintos escenarios.

Por ejemplo, en situaciones donde no se disponga de interfaz gráfica, una herramienta que se ejecute desde línea de comandos puede ser la única y mejor opción para obtener el volcado de datos, aunque sea más lenta que otra que solo está disponible con interfaz gráfica, pues la incompatibilidad de esta última la convierte automáticamente en la peor opción disponible, por muy rápida y eficiente que sea. Las características secundarias que se tendrán en cuenta en la comparativa son las siguientes.

- Portabilidad. Es la capacidad que posee una herramienta de poder ser transportada entre equipos. Las herramientas más portables son las que se pueden ejecutar simplemente colocando un ejecutable en el equipo, por ejemplo a través de una unidad de almacenamiento externa como un pendrive.
- Tamaño total de la herramienta. El tamaño total que ocupa la herramienta una vez instalada o extraída en el equipo. Se tiene en cuenta el espacio en el equipo antes y después de la instalación o extracción, así como el tamaño de la carpeta principal de instalación en el caso de una herramienta instalable.
- Tipo de licencia. Si una aplicación es de tipo comercial, si se trata de un software open source o es freeware. El tipo de producto es una característica a tener en cuenta, pues muchas veces el presupuesto es limitado y no se tiene acceso a las herramientas software propietarias, que son muy caras. También existen opciones de software libre con código abierto que garantizan más seguridad al poder analizar el código y que no se hayan introducido modificaciones en el mismo.
- Funcionalidades adicionales. En este apartado se analizarán todas las posibles funcionalidades que contenga la aplicación que no sean la adquisición de información de la memoria RAM. Por ejemplo, si una aplicación dispone de una herramienta para, una vez capturada la memoria, analizarla, se tratará de una funcionalidad adicional.
- Experiencia de usuario. La herramienta debe ser fácilmente utilizable por cualquier usuario, y tener las opciones disponibles de forma clara y visual. En este apartado se incluye, además, la facilidad de navegación por los menús, si los tiene, y la ayuda que se proporciona al usuario, por ejemplo, con el comando *-h*, si se trata de una herramienta que se ejecuta por línea de comandos.

Además de diferenciarse en características concretas, las herramientas que se van a analizar se distinguen también según su compatibilidad con el sistema operativo en el que se utilizan. El análisis comparativo de herramientas se centrará en los dos principales sistemas operativos más extendidos en la actualidad, Windows 10 y Linux, siendo Ubuntu 20.10 la distribución que representa al entorno Linux.

Con estas características, se procederá al análisis individual de cada herramienta. En este análisis se incluirá una breve descripción de la misma, así como una lista detallada de cada característica principal y secundaria para después poder comparar todas las herramientas entre sí. A continuación, se realizará una prueba de adquisición de datos de la memoria RAM con cada herramienta, empleando software de monitorización de tiempo para obtener los resultados más precisos posibles. Por último, con este tiempo de ejecución y la información de las características evaluadas, se generará una tabla en la que se mostrará, de manera rápida y visual, la comparativa entre todas las herramientas analizadas en esta tesis.

4.2. Entorno de pruebas

Las pruebas de adquisición de información de memoria RAM se realizarán en un entorno de pruebas controlado y bien definido, donde se incluyen tanto elementos software como hardware. Los elementos hardware y software que forman este entorno son las siguientes.

4.2.1. Hardware

- Ordenador de sobremesa. Equipo principal en el que se instalarán las herramientas y se realizarán las pruebasComponentes.
    - **CPU:** AMD Ryzen 7 3700x
    - **RAM:** 16GB DDR4 3200MHz
    - **Tarjeta Gráfica:** Nvidia RTX 3060 Ti
    - **Fuente de alimentación.**
    - **Almacenamiento:** 1TB SSD M.2 + 1TB HDD
    - **Sistema operativo:** Windows 10 versión 21H2 (Windows 11 insider build).
    - **Periféricos de entrada:** Ratón y teclado.

- Dispositivo USB 3.0 con 16 GB de almacenamiento. Algunas herramientas portables se iniciarán desde un USB para comprobar su funcionamiento en un medio extraíble y la diferencia de velocidad respecto a tenerla instalada en el equipo.

4.2.2. Software

- Sistemas operativos Windows 11 y Ubuntu 20.10. Los sistemas operativos en los que se probarán todas las herramientas de esta comparativa.

- Herramientas de adquisición de memoria RAM. Todas las herramientas que se evaluarán en la comparativa, incluyendo las compatibles con Windows 10 y las compatibles con Ubuntu 20.10.

    - **FTK Imager**
    - **OSForensics**
    - **WinPMem**
    - **Belkasoft RAM Capturer**
    - **Winen (EnCase)**
    - **Win64dd (Moonsols Windows Memory Toolkit)**
    - **Magnet RAM Capture**
    - **LiME**
    - **Memdump**
    - **Fmem**

- Oracle VM Virtualbox 6.1.22. Software utilizado para montar una máquina virtual con Ubuntu 20.10 dentro de Windows 10, y probar las herramientas exclusivas de este sistema operativo.

- Cronómetro de Windows y comando time de Ubuntu. Estas son las herramientas elegidas para realizar una comparativa objetiva y real de los tiempos de captura de la memoria

RAM, siempre y cuando la herramienta no cuente con alguna forma propia de calcular el tiempo, en ese caso se utilizará esa medida.

4.3. Metodología de evaluación

Para realizar una correcta evaluación de las herramientas y que la comparativa sea objetiva, eficaz y confiable, se seguirá una metodología bien definida que se aplicará a todos los análisis de herramientas de esta comparativa. Esta metodología se compone de la siguiente serie de pasos.

1. Descripción de la herramienta. En este apartado del análisis se describirá la herramienta según la definen sus creadores. También se indicarán de forma general las características que posee la herramienta y sus usos principales.

2. Prueba real de adquisición de datos. Se realizará una prueba real en la que se extraerán los datos de la memoria RAM con la herramienta en cuestión. Durante la realización de esta prueba se medirá el tiempo de ejecución y el consumo de recursos, de forma que se puedan evaluar las características principales de la comparativa. Para medir el impacto en los recursos de una manera más aproximada, se cerrarán todas las aplicaciones que no tengan que ver con la extracción de datos, como el navegador y otras aplicaciones en segundo plano que consumen recursos.

   Esta prueba se repetirá un total de tres veces para evitar causas puntuales que puedan influir en la adquisición, ralentizándola o acelerándola. Con las tres pruebas se calculará la media de tiempo y se tomará como la duración definitiva. Además, como el equipo de pruebas está formado por dos discos duros, uno de tipo SSD y otro de tipo HDD, las tres pruebas se medirán escribiendo datos en el disco HDD. Generalmente, salvo que se indique en la captura, las herramientas estarán instaladas en el SSD. Para comprobar cuánto tiempo de diferencia hay entre la escritura en HDD y SSD, se realizará una cuarta prueba en la que se escribirá la adquisición en el disco duro de estado sólido.

3. Análisis de características secundarias. Después de las características principales, se analizarán las funcionalidades adicionales de la herramienta tal y como se han descrito en el apartado de características secundarias.

4. Conclusiones y valoración de la herramienta. Por último, se resumirán las características evaluadas de la herramienta y se dará una valoración en base a esas características, indicando ventajas y desventajas de cada una.

5. Herramientas de Windows

El primer grupo de herramientas que se analizará será el formado por las utilidades que son compatibles con el sistema operativo Windows 10 en su versión 21H2, el cual corresponde a la versión insider de Windows 11. Se trata de un total de siete herramientas, donde se incluyen desde suites forenses como FTK Imager y OSForensics, hasta simples ejecutables como WinPmem o Winen. A continuación se analizarán cada una de las siete herramientas por separado, para después compararlas entre sí.

5.1. FTK Imager

La primera herramienta que se va a analizar es Forensic ToolKit Imager en su versión 4.5.0.3, lanzada en octubre de 2020.

5.1.1. Descripción

FTK Imager es una suite forense propiedad de la empresa AccessData [15]. Es una herramienta que se utiliza para la obtención y previsualización de evidencia electrónica. Su funcionalidad principal es la de realizar una captura forense completa de un medio de almacenamiento físico del equipo, lo que significa que se trata de una copia perfecta bit a bit sin realizar ningún cambioen el medio. Una vez obtenida la copia, la herramienta permite la visualización de la informaciónde forma reducida, con el objetivo de proporcionar los datos suficientes para decidir si seguir conla investigación utilizando otra herramienta forense más completa y específica para el análisis de evidencias. Por lo tanto, esta herramienta es muy utilizada en la extracción de datos de la memoria RAM, ya que asegura que se realizará una copia exacta de la memoria física sin modificaciones, de forma que se pueda utilizar después en un procedimiento forense.

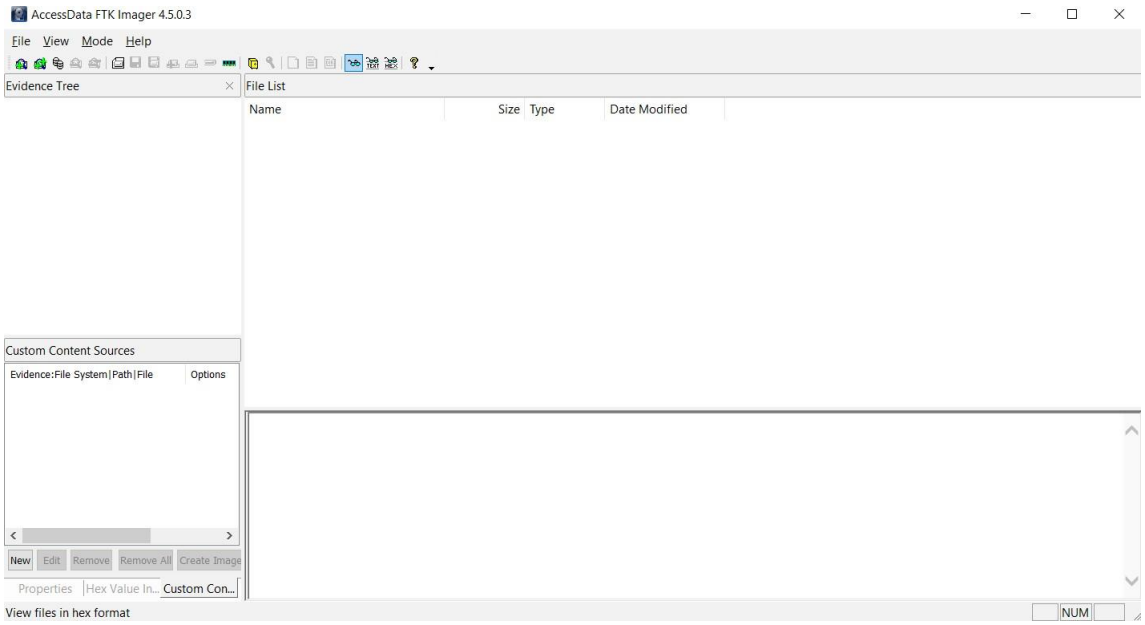


Figura 3. Ventana principal de FTK Imager.

Para capturar la memoria en esta herramienta se pueden utilizar dos formas. Una, desde la ventana principal se selecciona la opción *File -> Capture Memory*. La segunda, desde la ventana principal, en la barra de iconos superior, se selecciona la imagen que es una memoria RAM. Después de utilizar cualquiera de las dos opciones, se mostrará una ventana en la que se especificará una ruta

de guardado de la captura, el nombre con el que se almacenará y otras opciones como incluir el archivo de paginación, o crear un fichero AD1.

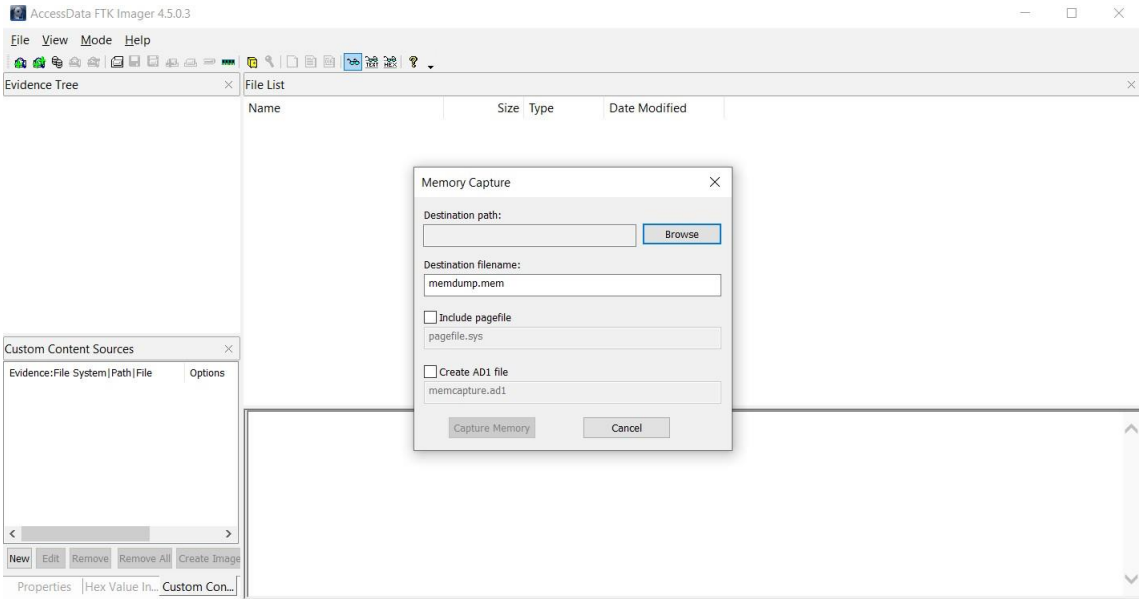


Figura 4. Ventana de captura de memoria de FTK Imager

Una vez capturada la memoria en el equipo, el cual dispone de 16 GB de memoria física instalada, se crea un archivo de volcado que ocupa un total de 16,4 GB.

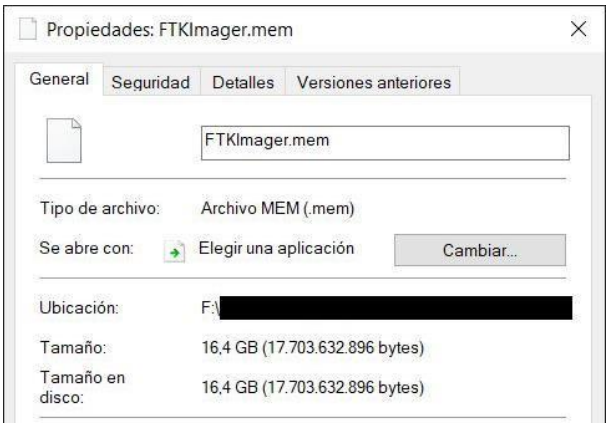


Figura 5. Tamaño captura de la memoria en FTK Imager

5.1.2. Características principales

En este apartado se analizarán las características principales en el software FTK Imager.

5.1.2.1. Velocidad de obtención del volcado de datos.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **2 minutos y 34 segundos**, con un margen de error de 1 segundo, entre que se realiza el cambio de ventana y se inicia y se para el contador.

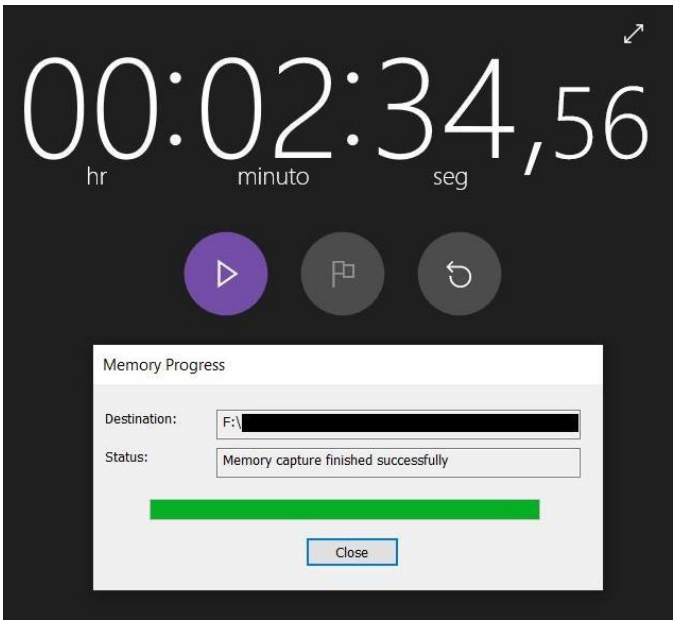


Figura 6. Primera captura con FTK Imager

En la **segunda prueba**, el tiempo ha sido de **2 minutos y 20 segundos**, con el mismo margen de error, lo que supone una rebaja de 14 segundos en el tiempo de adquisición.

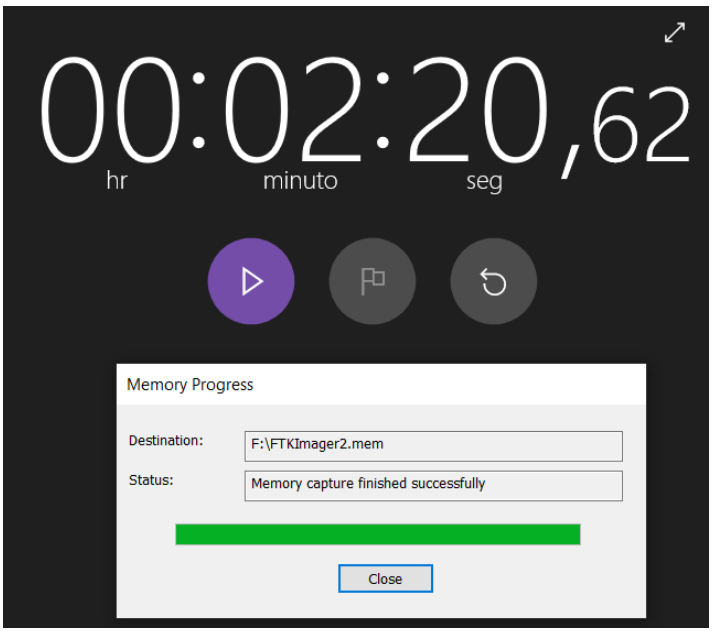


Figura 7. Segunda captura con FTK Imager

En la **tercera prueba**, el tiempo ha sido de **2 minutos y 33 segundos**, con el mismo margen de error, lo que la sitúa cerca de la primera prueba, pero lejos de la segunda.

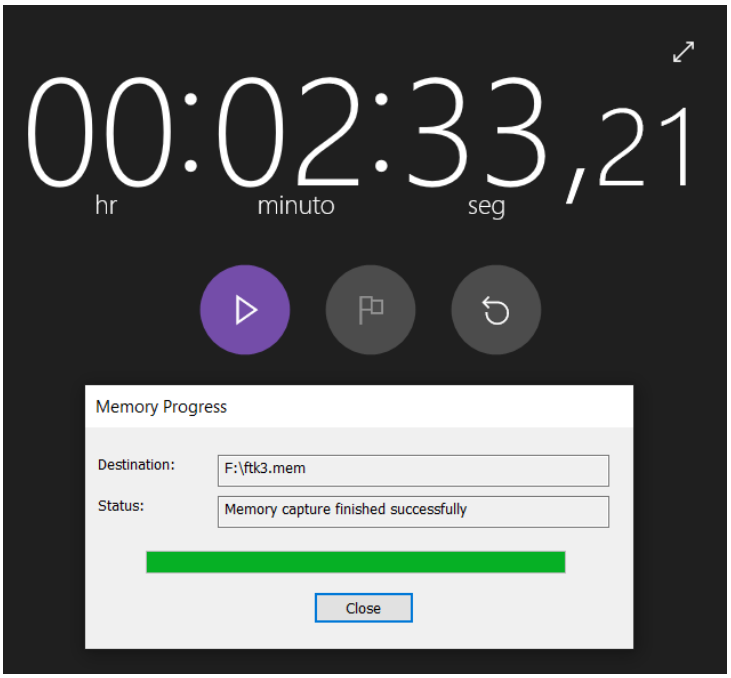


Figura 8. Tercera captura con FTK Imager

La media de **duración de captura en HDD** para la **herramienta FTK Imager** es de **2 minutos y 29 segundos**, con un margen de error de 1 segundo.

Por último, en la **prueba con SSD**, el tiempo ha sido de **36 segundos**, con el mismo margen de error que en las últimas pruebas. La diferencia con la captura en HDD es de 1 minuto y 53 segundos.

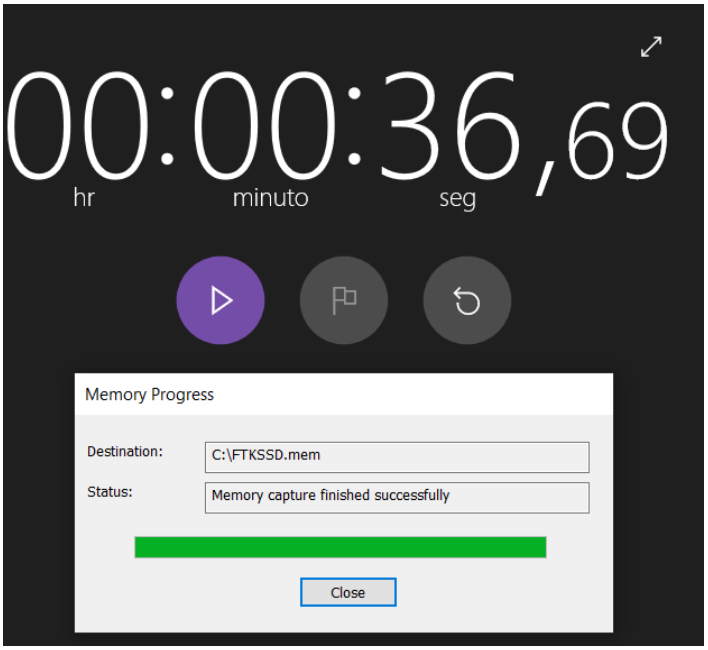


Figura 9. Captura con SSD en FTK Imager

5.1.2.2. *Impacto en el rendimiento del equipo*

Durante la captura, el rendimiento del equipo apenas se ha visto afectado por la herramienta. En el administrador de tareas, la aplicación FTK Imager utiliza durante las tres pruebas de HDD de esta adquisición, una media de 2.5% de tiempo de CPU y 15 MB de memoria RAM. El factor que más afecta sin duda es el uso del disco duro, el cual se mantiene en una media de 110 MB/s durante las capturas.

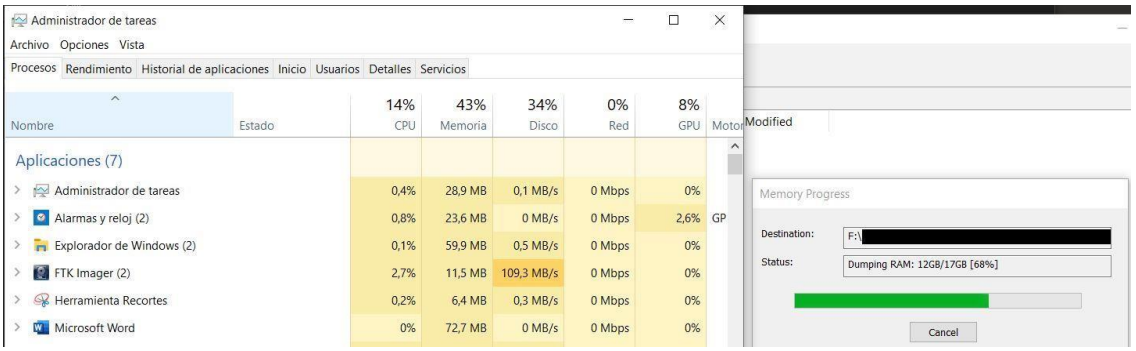


Figura 10. Impacto en el rendimiento HDD en FTK Imager

Sin embargo, en la prueba de SSD, el rendimiento del equipo ha variado. Ahora, la utilización de CPU ha aumentado hasta una media de un 8,5%, y la memoria se ha mantenido en 15MB. Pero donde se nota más diferencia es en el consumo de recursos del disco, que ha pasado a una media de 417 MB/s. Esta velocidad es cuatro veces más que la de adquisición en HDD, lo que muestra la mayor capacidad de procesamiento y rapidez de un SSD, que puede utilizar los recursos del equipo como la CPU de forma más eficiente para acelerar la captura.

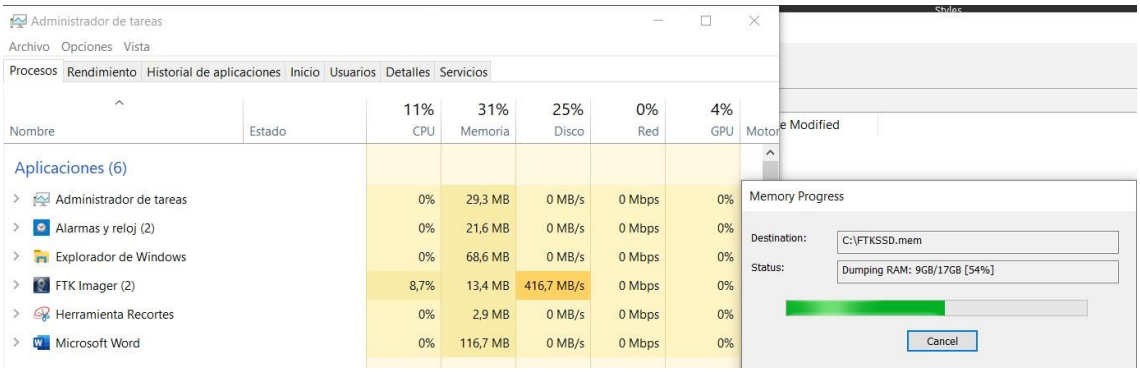


Figura 11. Impacto en el rendimiento SSD en FTK Imager

5.1.2.3. *Opciones adicionales de captura*

FTK Imager dispone de dos opciones adicionales de captura: incluir el archivo de paginación de memoria del sistema, y añadir un fichero en formato AD1. El archivo de paginación es un método que utiliza Windows a modo de reserva de memoria volátil cuando se sobrepasa la memoria física [16]. Por otro lado, el archivo AD1 (Access Data 1) se trata de un tipo de archivo exclusivo de esta herramienta y que permite analizar la captura posteriormente con la herramienta Forensic ToolKit, también propiedad de Access Data.

5.1.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta la herramienta FTK Imager.

5.1.3.1. Portabilidad

FTK Imager requiere de instalación previa para poder funcionar correctamente. La herramienta viene contenida en un instalador, el cual requiere permisos de administrador para su instalación. Sin embargo, aunque requiera de instalación, se puede elegir instalar la herramienta en una unidad de almacenamiento extraíble, como un USB, y realizar la captura desde allí. No obstante, realizar la captura desde esta unidad de almacenamiento extraíble conlleva una pérdida significativa de rendimiento, con una duración de captura de memoria superior a los 5 minutos.

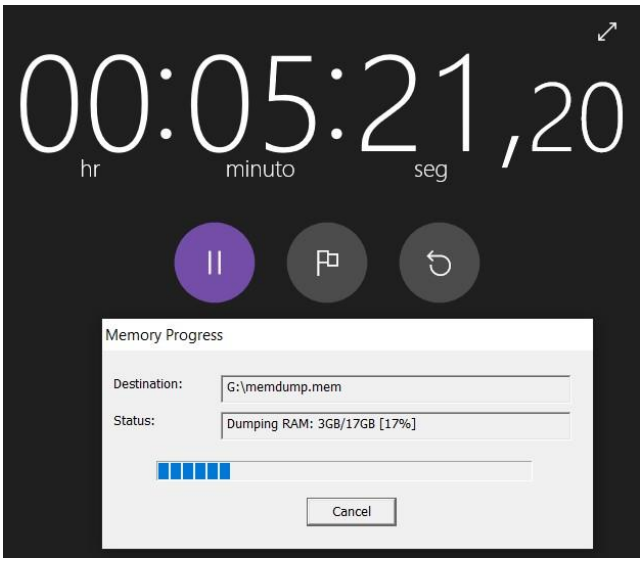


Figura 12. Captura con memoria USB en FTK Imager

5.1.3.2. Tamaño total de la herramienta

Como se ha indicado en el apartado de portabilidad, simplemente con el ejecutable de instalación sirve para poder instalar la herramienta en cualquier dispositivo. Este ejecutable ocupa un tamaño de 54,7 MB.

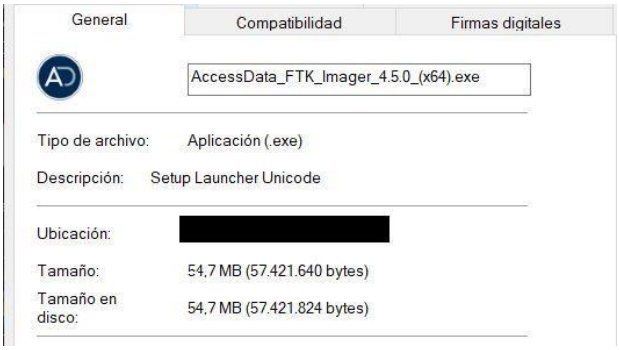


Figura 13. Tamaño instalador de FTK Imager

Por otra parte, una vez instalada la herramienta al completo, el tamaño de la carpeta donde se almacenan todos los archivos necesarios para su ejecución asciende hasta los 112 MB.

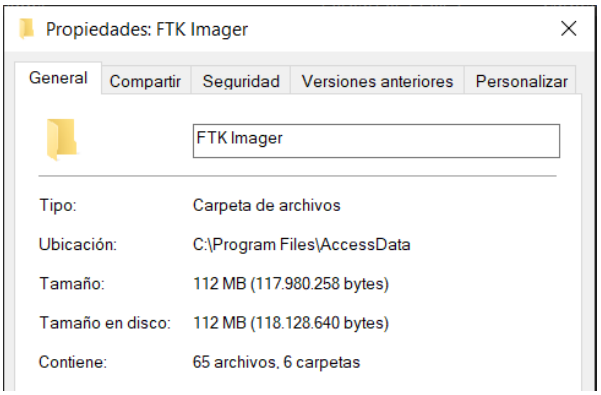


Figura 14. Tamaño total herramienta FTK Imager

Este tamaño es bastante grande para una herramienta de adquisición de memoria RAM. Sin embargo, hay que tener en cuenta que no se trata únicamente de una herramienta para capturar memoria, sino que esta es solo una de las opciones de las que dispone esta herramienta, siendo su principal funcionalidad la de visualizar datos de capturas de medios de almacenamiento como discos duros e imágenes del sistema.

5.1.3.3. Tipo de licencia

Al ser una herramienta propietaria de la empresa Access Data, el tipo de licencia es comercial, aunque su utilización es gratuita. Para obtener una copia de FTK Imager, se debe acceder a la página oficial de Access Data, y seleccionar la versión que se desee descargar. Una vez seleccionada, se debe completar un pequeño formulario en el que se solicitan algunos datos del interesado, como nombre y apellidos, puesto actual, sector en el que trabaja, país de residencia y correo electrónico, el dato más importante, pues el enlace para descargar la herramienta se enviará por correo a la dirección indicada tras el cumplimiento del formulario.

5.1.3.4. Funcionalidades adicionales

Como suite de visualización de evidencias digitales, FTK Imager dispone de multitudes funcionalidades adicionales a la captura de datos de la memoria RAM. La principal funcionalidad de esta herramienta se basa en añadir evidencias digitales en forma de imágenes de dispositivos y analizar su contenido. Además, una opción muy útil de FTK Imager es la de montar todos los dispositivos conectados al equipo en ese momento.

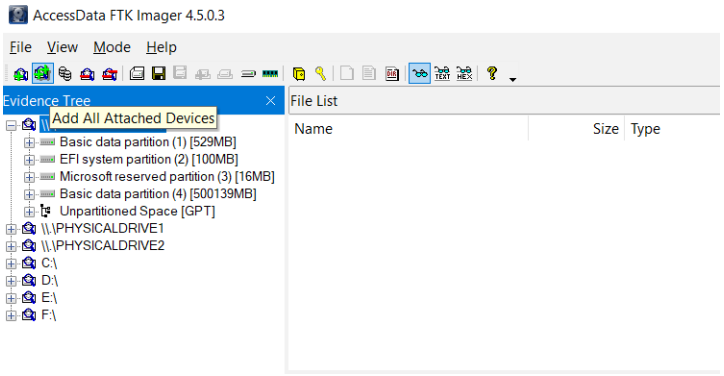


Figura 15. Opción montar dispositivos conectados en FTK Imager

Una vez seleccionada la opción, se mostrarán en el árbol de evidencias todos los dispositivos conectados al equipo, de forma que se pueda buscar información en ellos a continuación. ÇAl seleccionar un fichero, se muestra una vista hexadecimal y su traducción en ASCII, que proporcionan mucha información relevante sobre el archivo. Esta funcionalidad puede resultar muy útil en el análisis forense de un equipo, pues puede mostrar todos los dispositivos y analizar datos relevantes desde el punto de vista forense como por ejemplo la tabla MFT de un disco NTFS.

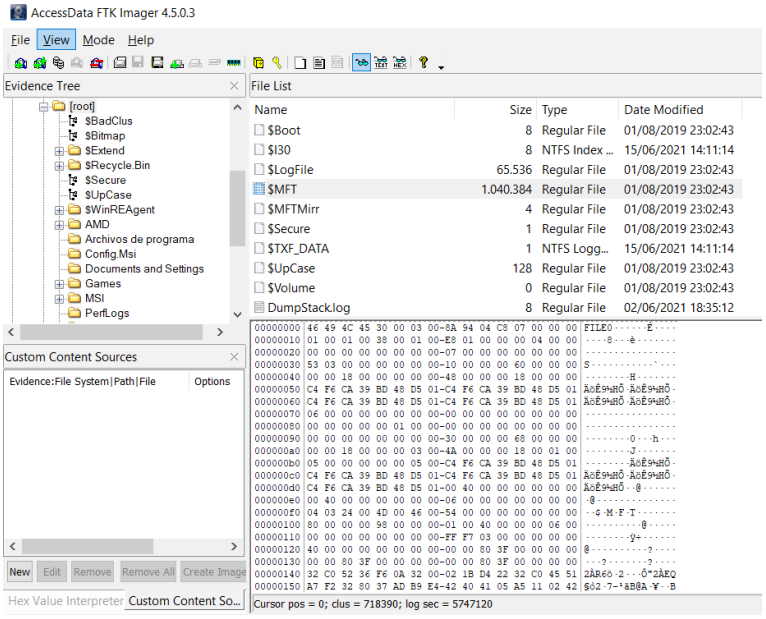


Figura 16. Vista hexadecimal de la tabla MFT

Otra opción muy interesante es la de crear una imagen de un disco. Aquí se puede seleccionar el medio que se va a duplicar, como un disco físico, una archivo de imagen (como un archivo ISO), o incluso el contenido de una carpeta, aunque esta última opción no es muy efectiva, ya que solo duplica archivos lógicos, y no incluye datos como espacio no asignado, ficheros eliminados o metadatos.

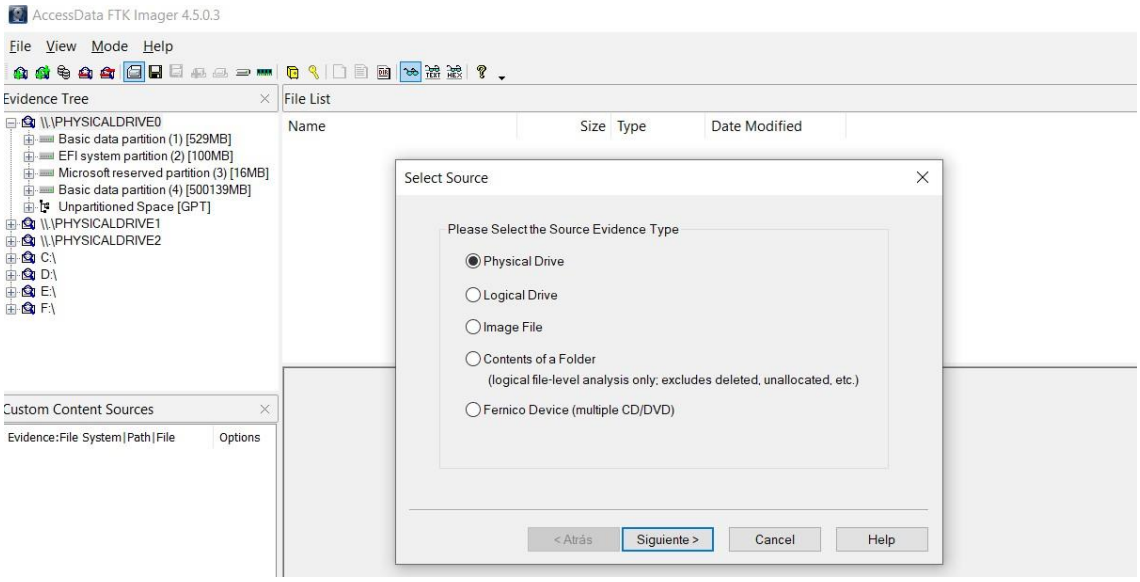


Figura 17. Crear imagen de un disco en FTK Imager

Otras opciones secundarias que proporciona FTK Imager es la posibilidad de volcar los archivos protegidos de un dispositivo en una ruta del equipo, para su posterior análisis. También se puede detectar la encriptación EFS de una evidencia, que es una tecnología exclusiva de sistemas NTFS 3.0 para trabajar con ficheros encriptados de forma transparente al usuario [17].

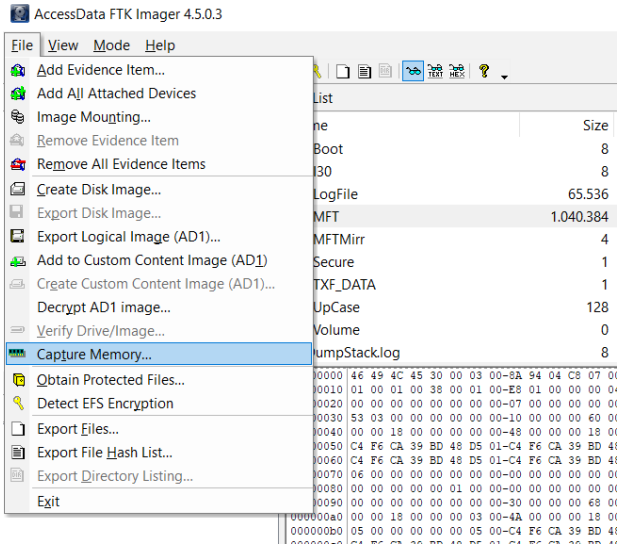


Figura 18. Opciones adicionales de FTK Imager

Por último, FTK Imager permite trabajar con ficheros en formato AD1, ya mencionado en el apartado de características de captura de memoria, permitiendo su desencriptación. También se puede exportar una imagen a este tipo de formato para trabajar en la herramienta Forensic ToolKit.

5.1.3.5. Experiencia de usuario

Al tratarse de una herramienta con interfaz gráfica, FTK Imager es más visual y fácilmente utilizable que otras que se ejecutan por terminal. Para poder realizar la captura de la memoria simplemente se sigue el asistente de captura, permitiendo seleccionar las opciones necesarias de

forma simple y visual, sin necesidad de conocer los parámetros que las habilitan. No obstante, si se desea conocer la herramienta más en profundidad, se puede acceder a la guía de usuario disponible. Al seleccionar el icono del interrogante en la barra de iconos superior en la ventana principal de FTK Imager, se abrirá un documento PDF que contiene toda la información necesaria para trabajar correctamente con la herramienta.

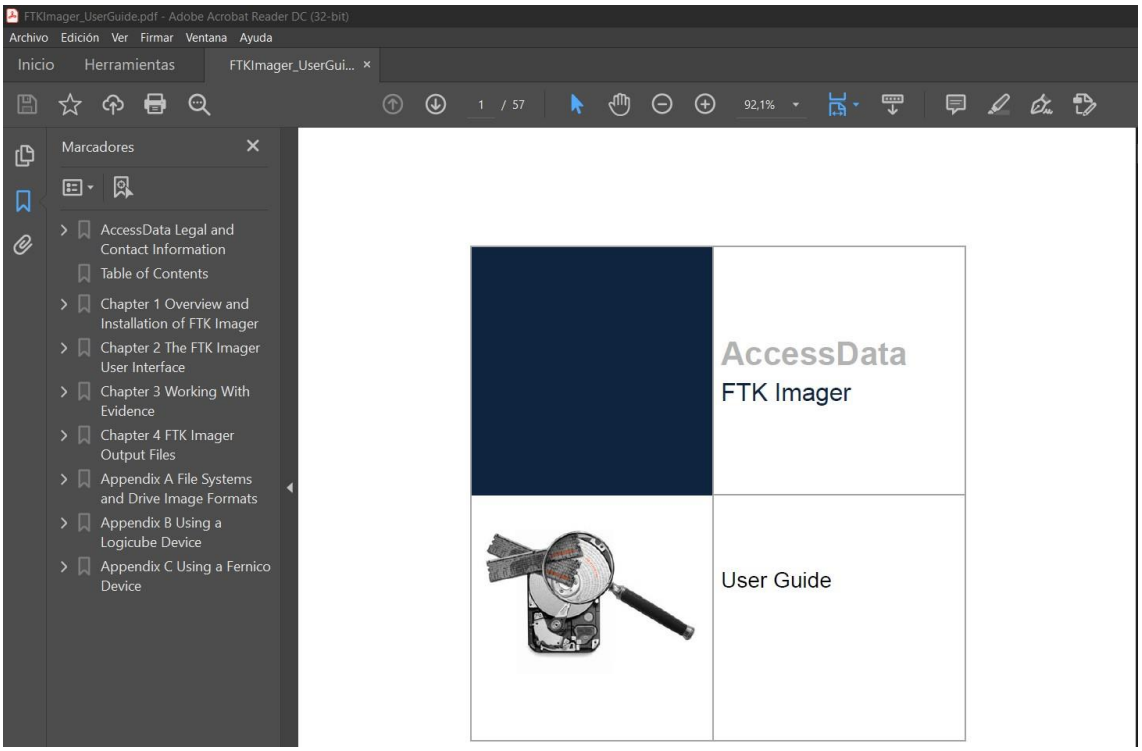


Figura 19. Guía de usuario de FTK Imager

La guía está bien estructurada en capítulos, por lo que se puede saltar a la parte que interese aprender rápidamente. Además, incluye multitud de capturas en las que visualizar las opciones que se explican. Un punto negativo de esta guía es que solamente está disponible en idioma inglés, lo que reduce su difusión y su accesibilidad a otros usuarios.

5.1.4. Conclusiones

La herramienta FTK Imager es una suite forense que permite capturar memoria, aunque su principal funcionalidad es la de visualizar evidencias digitales. En cuanto a adquisición de datos de memoria RAM, la herramienta es bastante rápida, consiguiendo una captura completa en 2 minutos y 33 segundos de media para un disco duro habitual. Las funcionalidades adicionales que presenta la convierten en una de las mejores opciones para visualizar evidencias, y para capturar memoria la opción de crear un fichero AD1 que se pueda analizar posteriormente con la herramienta Forensic ToolKit es muy útil.

Ventajas: Velocidad de captura, visualización de evidencias.

Desventajas: Portabilidad.

Valoración final: 8/10.

5.2. OSForensics

La siguiente herramienta que se va a analizar se trata de OSForensics en su versión 8.0.1000, lanzada en octubre de 2020.

5.2.1. Descripción

OSForensics es una suite forense propiedad de la empresa PassMark, que permite identificar archivos y actividad sospechosa en un equipo, extraer la evidencia rápidamente y gestionar la investigación forense de forma centralizada [18]. Esta herramienta contiene una gran variedad de opciones para poder realizar análisis y obtención de evidencias digitales en un equipo, incluyendo la captura de datos de la memoria RAM mediante un volcado de datos. Entre sus múltiples funcionalidades se encuentra la identificación de archivos y actividad sospechosa en un equipo, utilizando herramientas que permitan verificar los hashes de los ficheros; identificar los cambios realizados en los archivos mediante una función de firma de disco duro, que garantiza la integridad de la evidencia; visualizando la línea temporal proporcionada por OSForensics sobre la actividad sobre un archivo determinado; o empleando alguna de las varias herramientas de análisis de ficheros, como un buscador SQLite, un visor de correo o un visor $UsnJrnl para ver las entradas de los cambios de un volumen NTFS, entre otras herramientas.

Adicionalmente a la investigación de ficheros, OSF permite la gestión adecuada y segura de la evidencia en una investigación, proporcionando los medios necesarios para crear casos personalizados a cada investigación, generando informes automáticamente en función a los resultados obtenidos, permitiendo la visualización y la duplicación de imágenes de evidencias digitales como discos duros, y creando un registro de auditoría de todos los pasos seguidos y herramientas utilizadas en el transcurso de la investigación.

Figura 20. Ventana principal de OSForensics

Para capturar la memoria del equipo en esta herramienta se selecciona la opción Memory Viewer en el panel lateral izquierdo "Workflow". Una vez seleccionada, se muestra la siguiente pantalla, con un mensaje de aviso sobre la visualización de memoria activa del sistema.

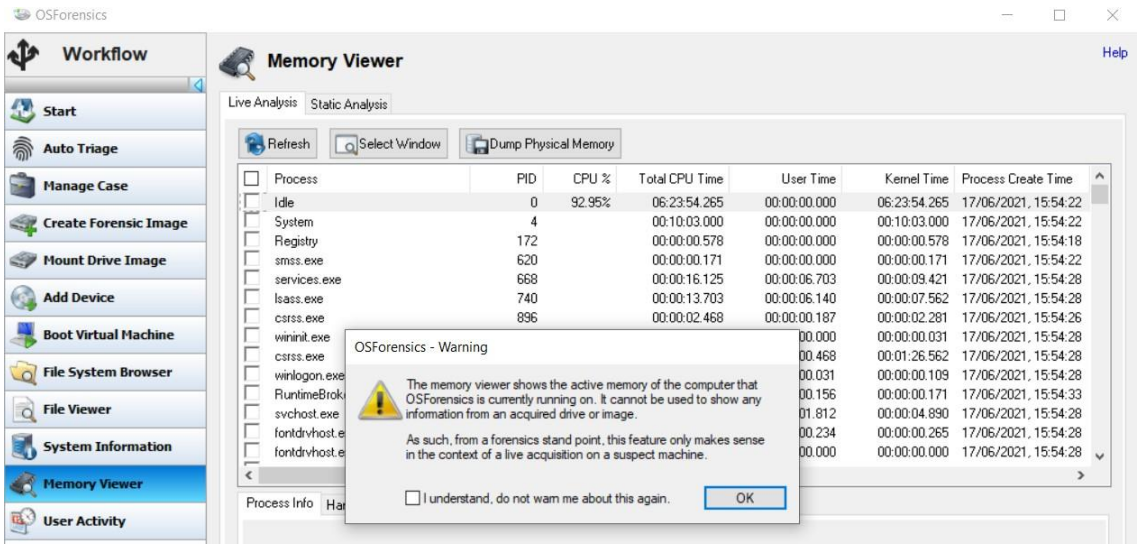


Figura 21. Visor de memoria en OSForensics

Para continuar a realizar una captura de la memoria física, se selecciona la opción Dump Physical Memory, en la parte superior de la pantalla. Una vez seleccionada la opción, se mostrará un explorador de archivos, en el que se indicará una ruta y un nombre con el que guardar la captura. Tras esto, OSF empezará con el volcado de datos en la ruta especificada. Una funcionalidad importante es que se muestra un tiempo aproximado de finalización de la captura, así como la velocidad actual de volcado de información, siendo esta actualizada en todo momento.

Al terminar, se podrá acceder al archivo creado y comprobar que efectivamente, vuelca todo el contenido de la memoria, 16,4 GB de tamaño total.

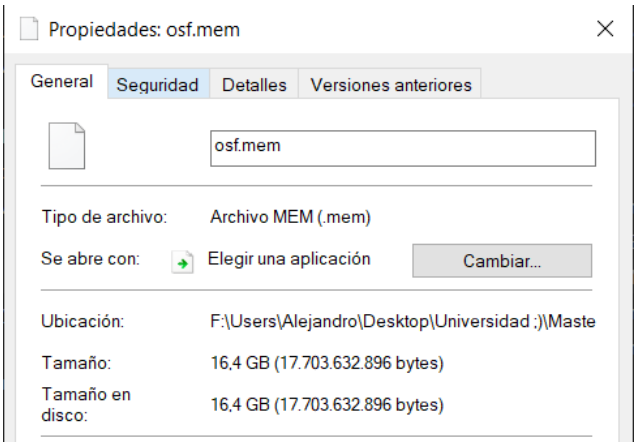


Figura 22. Tamaño captura de la memoria en OSForensics

5.2.2. Características principales

En este apartado se analizarán las características principales en el software OSForensics.

5.2.2.1. Velocidad de obtención del volcado de datos.

Nota: en las pruebas de velocidad con esta herramienta no se puede mostrar el mensaje de finalización de la captura, pues OSForensics no avisa de la finalización del volcado, por lo que el tiempo será aproximado y se tendrá en cuenta el tiempo cuando el mensaje se cierra, pero no podrá aparecer en las capturas de imagen que se muestran.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **3 minutos y 43 segundos**, con un margen de error de 3 segundos, entre que se cierra el mensaje de progreso y se inicia y se para el contador.

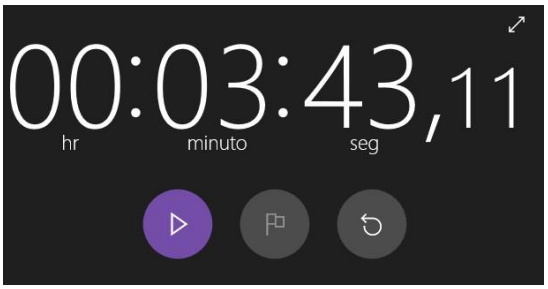


Figura 23. Primera captura con OSForensics

En la **segunda prueba**, el tiempo ha sido de **3 minutos y 35 segundos**, con el mismo margen de error, lo que supone una rebaja de 8 segundos en el tiempo de adquisición.

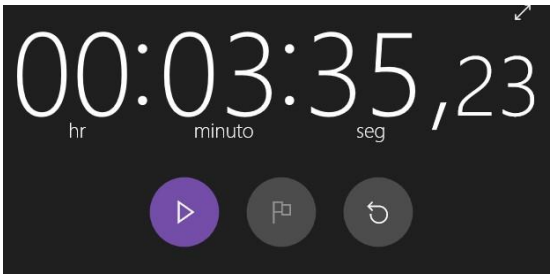


Figura 24. Segunda captura con OSForensics

En la **tercera prueba**, el tiempo ha sido de **3 minutos y 38 segundos**, con el mismo margen de error, lo que la sitúa entre medias de las dos primeras pruebas.

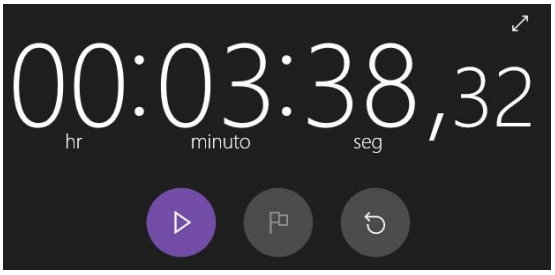


Figura 25. Tercera captura con OSForensics

La media de **duración de captura en HDD** para la **herramienta OSForensics** es de **3 minutos y 38 segundos**, con un margen de error de 3 segundos.

Por último, en la **prueba con SSD**, el tiempo ha sido de **47 segundos**, con el mismo margen de error que en las últimas pruebas, 3 segundos. La diferencia con la captura en HDD es de 2 minutos y 51 segundos.

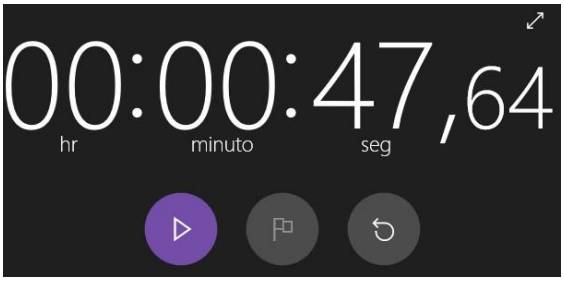


Figura 26. Captura con SSD en OSForensics

5.2.2.2. Impacto en el rendimiento del equipo

Durante la captura, el rendimiento del equipo apenas se ha visto afectado por la herramienta. En el administrador de tareas, la aplicación OSForensics utiliza durante las tres pruebas de HDD de esta adquisición, una media de 2,6% de tiempo de CPU y 55 MB de memoria RAM. El factor que más afecta sin duda es el uso del disco duro, el cual varía bastante, empezando en los 150 MB/s durante los primeros segundos de la captura, pero estabilizándose hacia los 77 MB/s durante el resto de la captura.

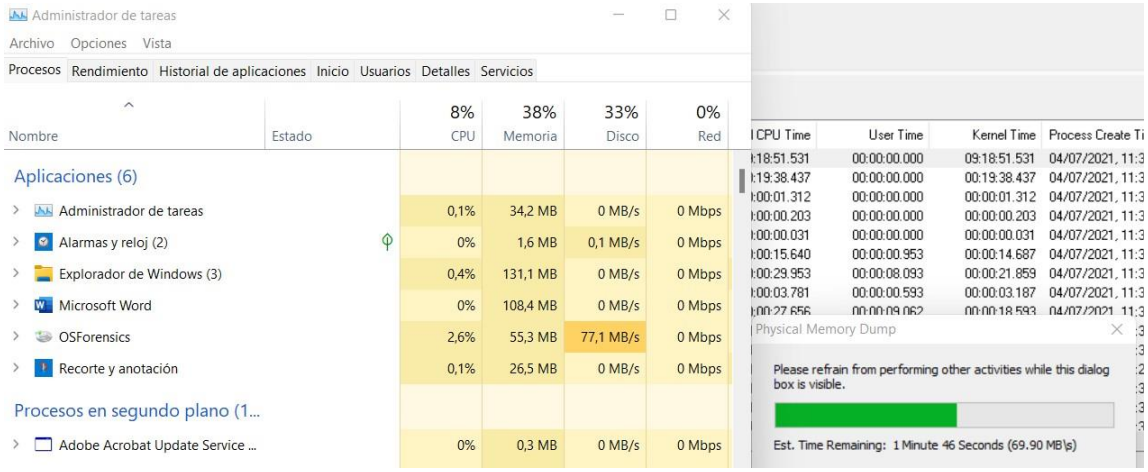


Figura 27. Impacto en el rendimiento HDD en OSForensics

En cuanto al impacto en el rendimiento en la prueba con SSD, la utilización de CPU ha aumentado hasta una media de un 8%, y la memoria se ha mantenido en los 56MB de la captura con HDD. Pero donde se nota más diferencia es en el consumo de recursos del disco, que ha pasado a una media de 417 MB/s, seis veces más que la de adquisición en HDD.

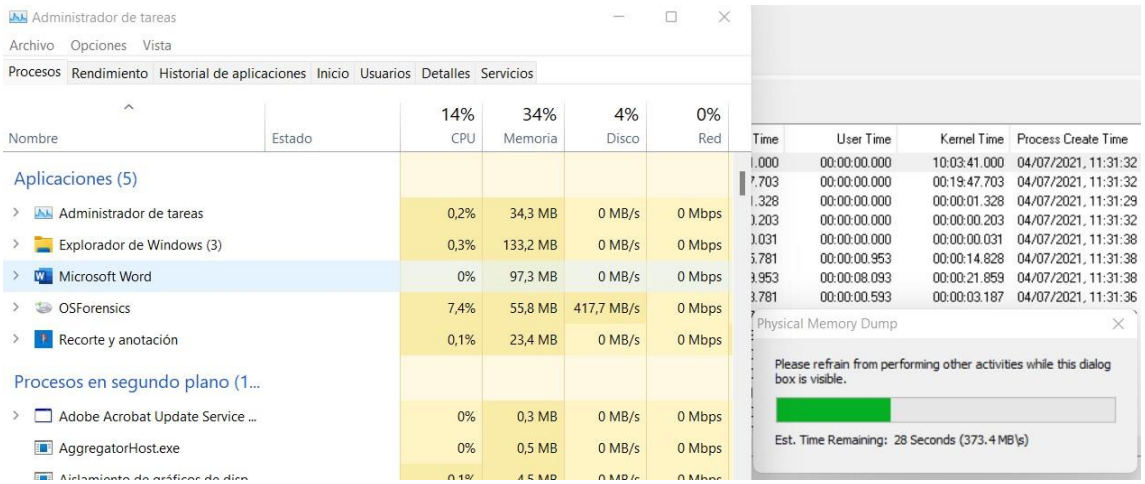


Figura 28. Impacto en el rendimiento SSD en OSForensics

5.2.2.3. Opciones adicionales de captura

OSForensics no dispone de ninguna opción adicional de captura, solamente permite el volcado completo de la memoria física del sistema. Esto es un punto negativo para la herramienta desde el punto de vista de la captura de información de la memoria RAM, pues no ofrece ninguna ventaja frente a otras herramientas especializadas en el volcado.

5.2.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta la herramienta OSForensics.

5.2.3.1. Portabilidad

OSForensics es una herramienta que requiere de instalación previa en el equipo para poder funcionar correctamente. Al igual que en el caso de FTK Imager, esta herramienta es una suite forense con multitud de módulos adicionales que no se relacionan con la captura de datos de la memoria RAM. Por esta razón, la portabilidad es bastante escasa: aunque es posible instalar la herramienta en una unidad externa como un pendrive USB, no es recomendable por la lentitud en ejecución de la adquisición de datos de la memoria. Para aprovechar al máximo la herramienta, se recomienda instalarla en un disco duro propio de la máquina, pues la variedad de opciones de las que dispone permite que sea utilizada más fácilmente cuanto más rápido se ejecuten.

5.2.3.2. Tamaño total de la herramienta

Como se ha indicado en el apartado de portabilidad, simplemente con el ejecutable de instalación sirve para poder instalar la herramienta en cualquier dispositivo. Este ejecutable ocupa un tamaño de 195 MB.

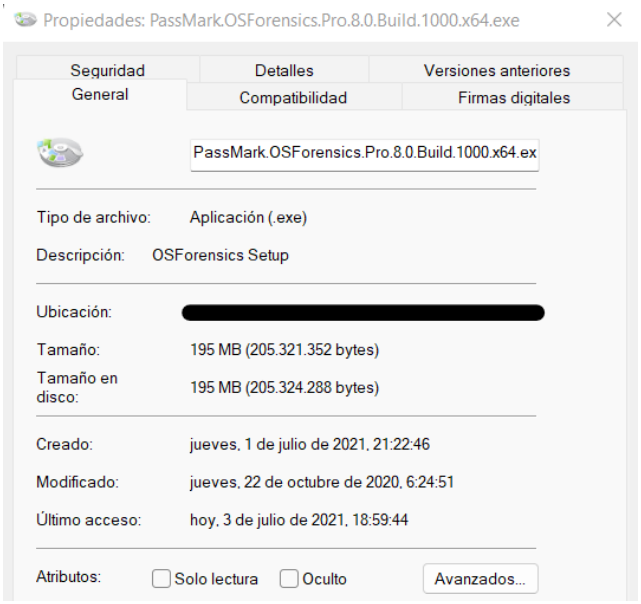


Figura 29. Tamaño instalador de OSForensics

Por otra parte, una vez instalada la herramienta al completo, el tamaño de la carpeta donde se almacenan todos los archivos necesarios para su ejecución asciende hasta los 396 MB.

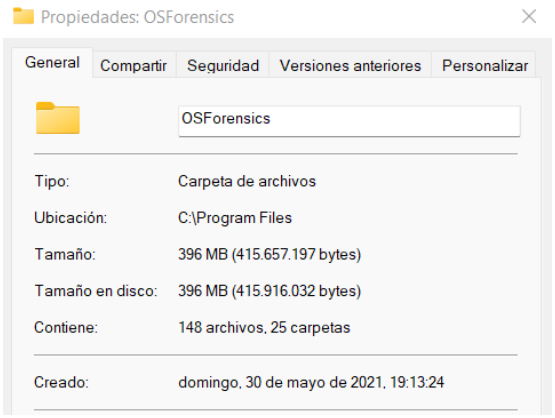


Figura 30. Tamaño total herramienta OSForensics

Este tamaño es demasiado grande para una herramienta de adquisición de memoria RAM, superando incluso a otras suites forenses como FTK Imager. Sin embargo, hay que tener en cuenta que no se trata únicamente de una herramienta para capturar memoria, sino que esta es solo una de las opciones de las que dispone esta herramienta, disponiendo de diversas opciones y módulos dentro de la misma que permiten realizar multitud de tareas forenses, incluyendo

5.2.3.3. Tipo de licencia

Al ser una herramienta propietaria de la empresa PassMark, el tipo de licencia es comercial, aunque se puede solicitar una prueba gratuita por 30 días. Para obtener la prueba gratuita de OSForensics, se debe acceder a la página oficial de PassMark, seleccionar el software OSForensics y la opción free trial (prueba gratuita). Una vez seleccionada, aparecerá una página con las distintas versiones del programa, pero la última aparecerá al comienzo de la página. Si se clica en la versión, comenzará la descarga del programa, sin necesidad de rellenar formularios ni introducir datos personales.

5.2.3.4. Funcionalidades adicionales

Las funcionalidades adicionales de esta herramientas son tantas y tan extensas que sería inabarcable explicarlas todas en un solo apartado. Por lo tanto, el estudio se centrará en nombrar las funcionalidades y módulos más relevantes de OSForensics.

Esta herramienta dispone de varios módulos relacionados con el análisis de la memoria RAM del equipo, incluyendo el ya mencionado proceso de volcado, agrupados en el apartado Memory Viewer. Antes de volcar la memoria, es posible visualizar todo el contenido en ejecución y presente en la memoria sin necesidad de crear un archivo volcado con los datos, lo cual es muy útil en equipos sospechosos en un incidente informático.

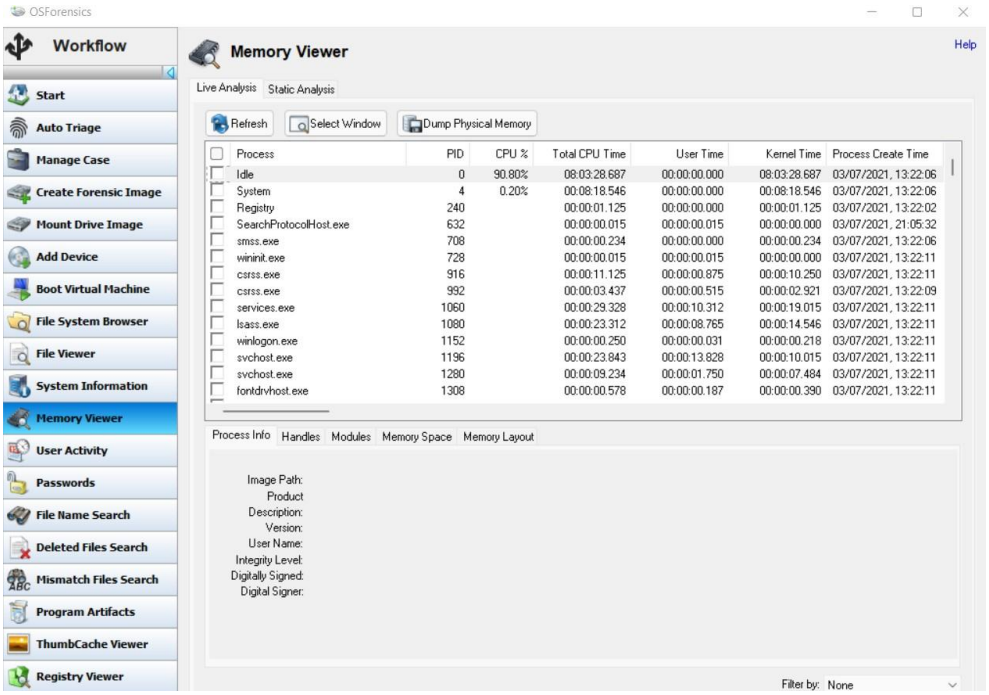


Figura 31. Módulo Memory Viewer de OSForensics

Además de este módulo, OSForensics permite el análisis de la memoria RAM extraída mediante la herramienta Volatility 3.0, la más conocida y utilizada en materia de análisis de memoria volátil, en su versión con interfaz gráfica, que dispone de menús con las distintas opciones de análisis de la memoria sin necesidad de conocer los comandos específicos. Además, se indican los pasos a seguir para trabajar con la herramienta, haciéndola muy accesible a cualquier usuario de la misma.

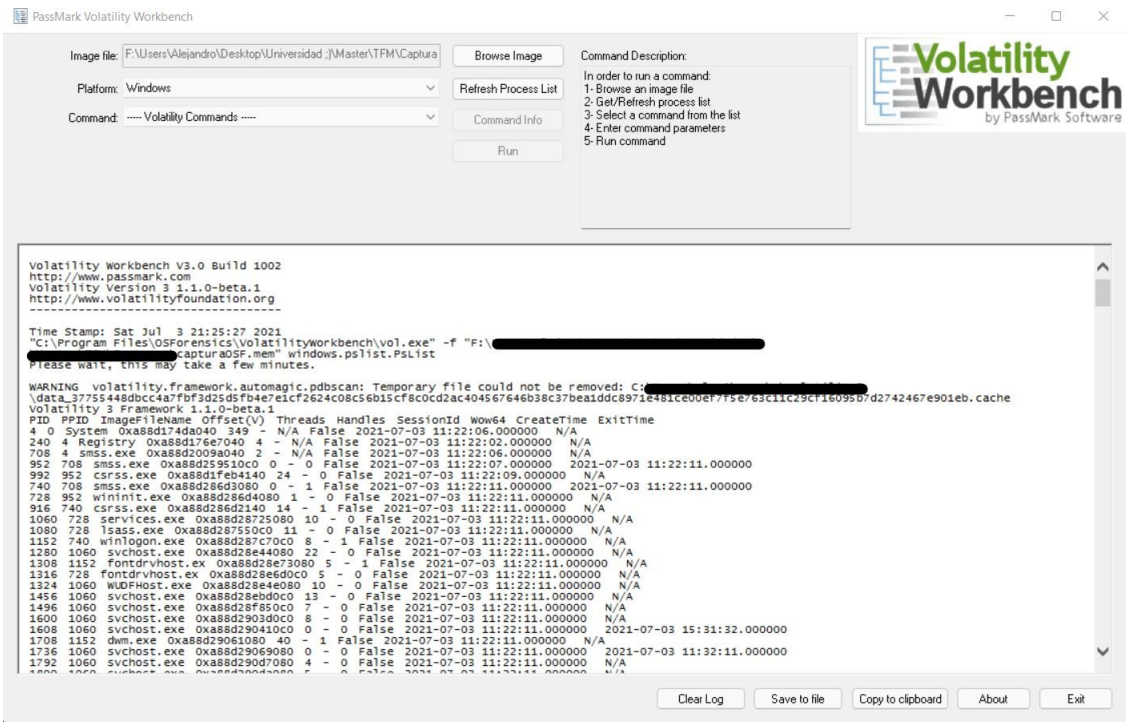


Figura 32. Módulo de Volatility 3.0 en OSForensics

Una característica importante de esta suite es que permite organizar las investigaciones en casos, de forma que las evidencias se mantienen agrupadas y separadas según el caso al que pertenezcan, con multitud de opciones de personalización de información sobre el caso y la investigación.

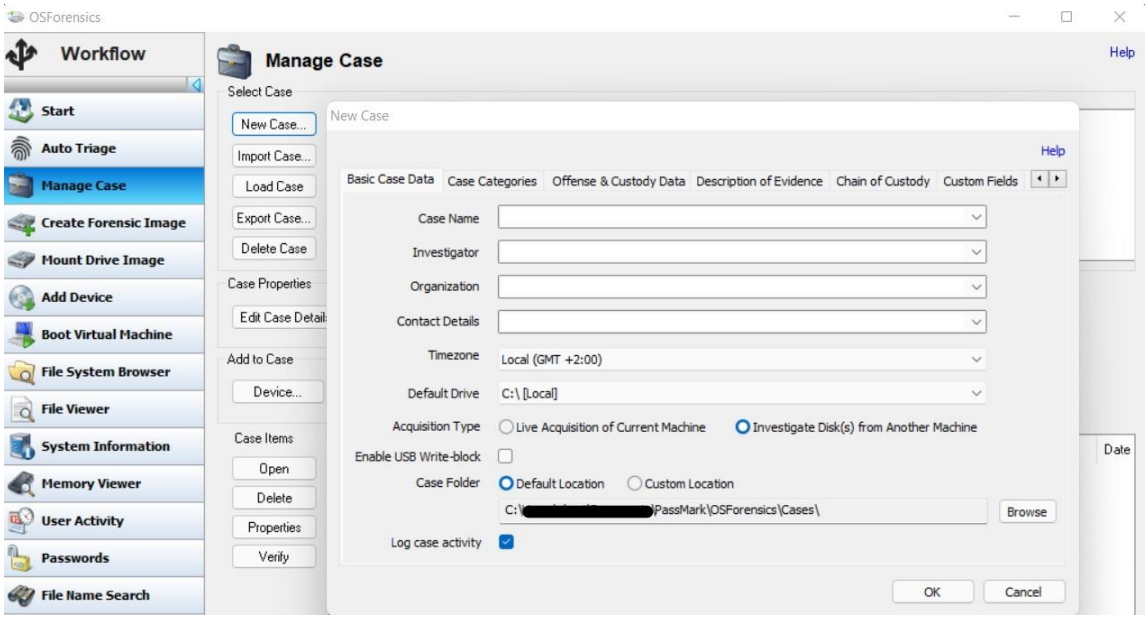


Figura 33. Creación de casos forenses en OSForensics

Pero la funcionalidad más interesante de OSForensics es la posibilidad de iniciar un escaneo completo de un disco duro o evidencia digital en vivo, indicando las opciones que va a escanear y analizar la herramienta. Estas opciones incluyen las evidencias más comunes que se suelen obtener y analizar en un análisis forense de un equipo, como la lista de procesos en ejecución, un volcado de la memoria física del sistema o encontrar archivos eliminados recientemente.

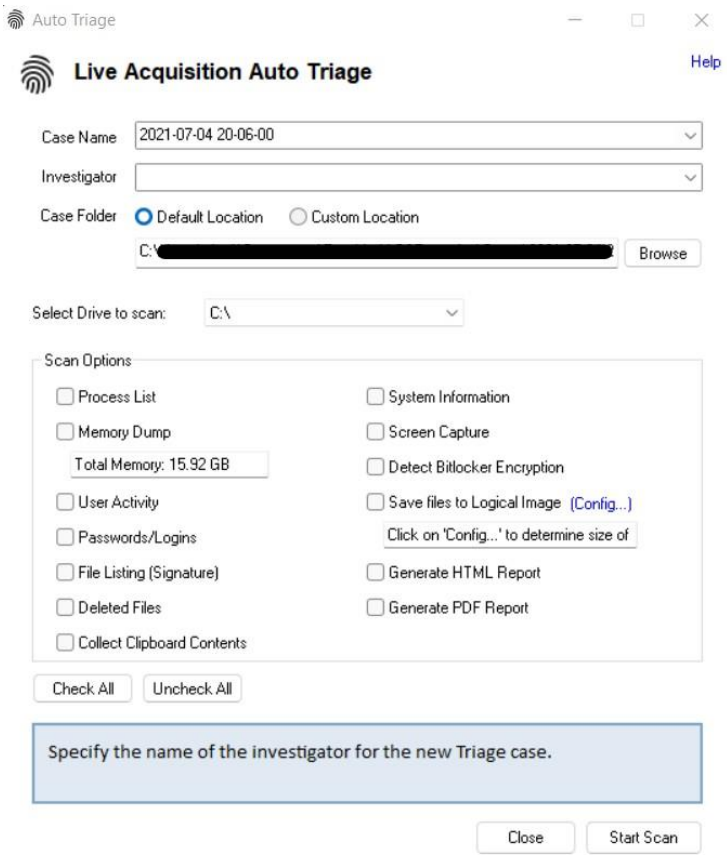


Figura 34. Opciones del escaneo en vivo de OSForensics

Además, al final del proceso, se dispone de la opción de generar un informe con los resultados del escaneo en formato HTML. Se puede acceder a este informe desde un navegador, y acceder a cada sección analizada en el escaneo, visualizando las evidencias recogidas por la herramienta. En algunos casos, como en el de los usuarios y contraseñas del equipo, la información se almacena en documentos CSV, para su análisis posterior con otras herramientas.

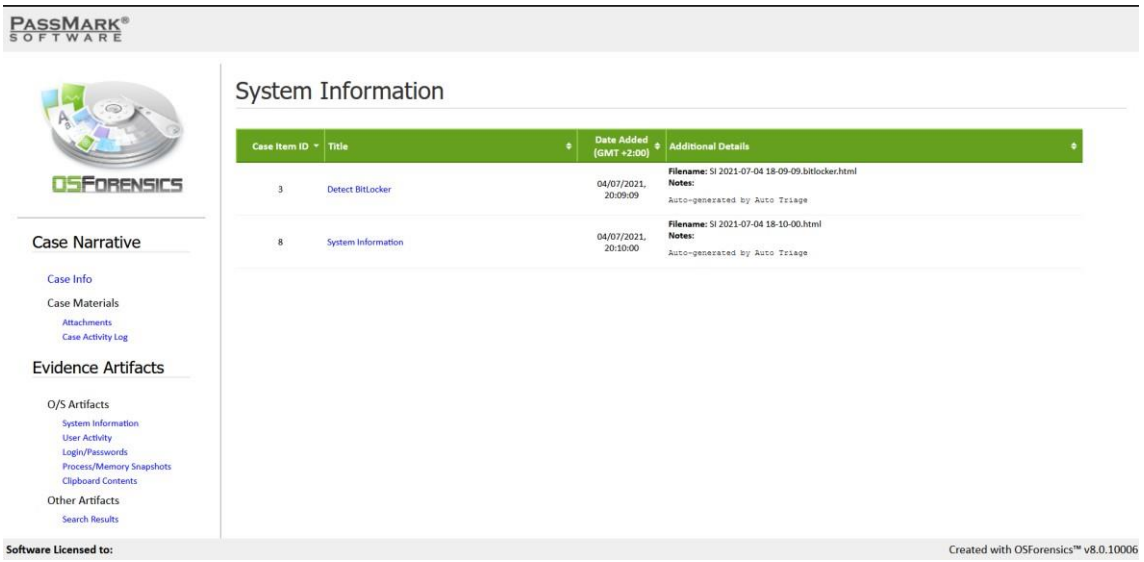


Figura 35. Informe HTML con los resultados del escaneo en vivo de OSForensics

5.2.3.5. Experiencia de usuario

Al tratarse de una herramienta con interfaz gráfica, OSForensics es más visual que otras que se ejecutan solamente a través de terminal. Los menús de la herramienta son muy visuales y los distintos módulos están bien organizados en el panel lateral izquierdo, con un acceso rápido a las distintas opciones que presenta esta herramienta. Asimismo, OSForensics dispone de una sección específica de ayuda al final de la pantalla de inicio, en la que se puede acceder a información sobre la herramienta, consultar la guía de ayuda al usuario, reiniciar OSForensics en modo debug, comprobar actualizaciones o contactar directamente con el soporte de PassMark en el caso de tener una licencia comercial comprada.

Figura 36. Apartado de ayuda de OSForensics

Si se desea conocer la herramienta y sus opciones más en profundidad, se puede acceder a la guía de ayuda al usuario, donde se abrirá una ventana con un panel que contiene toda la información necesaria para trabajar correctamente con la herramienta. Esta ayuda, disponible solamente en idioma inglés, contiene toda la información necesaria para trabajar correctamente y comprender todos los módulos y opciones adicionales que se incluyen en la herramienta, todo de forma visual con imágenes explicativas.

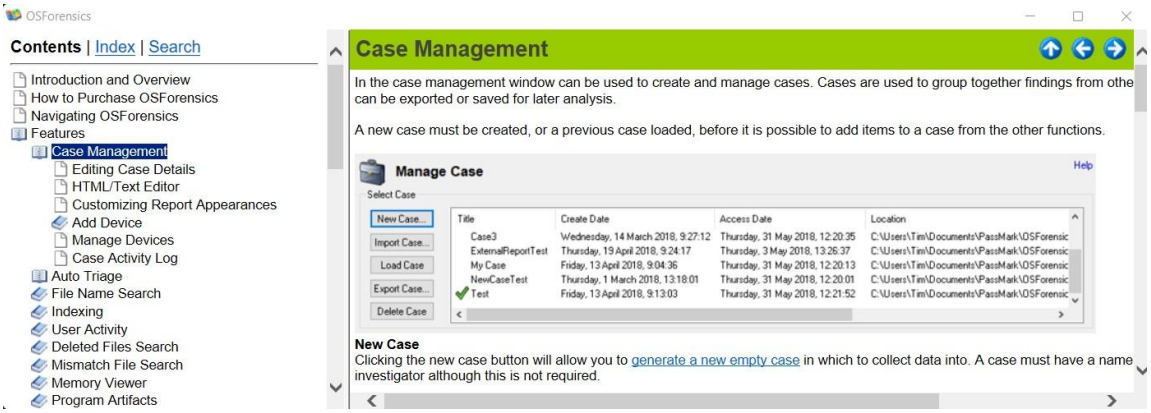


Figura 37. Guía de ayuda de OSForensics

5.2.4. Conclusiones

La herramienta OSForensics es una suite forense completa que permite capturar memoria, aunque disponga de multitud de opciones de análisis de evidencias digitales. En cuanto a la adquisición de datos de la memoria RAM, la herramienta es algo lenta, no aprovechando todo el ancho de banda del equipo para realizar la captura, ni siquiera en la prueba realizada con SSD, dando una velocidad de 3 minutos y 38 segundos de media para un disco duro habitual. Sin embargo, todas las funcionalidades adicionales que presenta la convierten en una de las mejores opciones para realizar trabajos de investigación forense, con las opciones de crear casos y generar informes de manera automática, así como la posibilidad de analizar la memoria tras extraerla sin necesidad de utilizar otro programa, gracias a Volatility Workbench. No obstante, este análisis se centra en la captura de memoria, y en este apartado la herramienta no ofrece funcionalidades adicionales que la hagan destacar respecto a otras opciones del mercado, sin incluir su exorbitado precio de licencia.

Ventajas: Herramientas forenses.

Desventajas: Velocidad de captura, portabilidad, licencia.

Valoración final: 6,5/10.

5.3. WinPMem

La siguiente herramienta que se va a analizar se trata de WinPMem, en su versión 4.0 RC2 lanzada en octubre de 2020.

5.3.1. Descripción

WinPMem es una herramienta de línea de comandos open source disponible en Windows, siendo la opción por defecto para capturar memoria durante mucho tiempo, como parte del proyecto Rekall, aunque ahora se ha desligado y existe de manera independiente en su propio repositorio de Github [19]. Es una herramienta escrita en código C, y desarrollada por el equipo formado por Mike Cohen, Viviane Zwanger y Matthias Braun, con agradecimientos a la comunidad DFIR. Inicialmente, el código se desarrolló en Google, pero ahora tiene licencia Apache, por lo que es completamente libre de uso y distribución. En cuanto a las características de la herramienta, esta dispone de 2 versiones diferentes, una para sistemas de 32 bits y otra para sistemas de 64 bits,

siendo esta última la utilizada en el análisis. Además, dispone de 3 modos diferentes e independientes de captura, soporte para volcados de memoria en bruto, y un dispositivo de lectura de interfaz que se utiliza en lugar de leer los datos directamente del kernel, lo que permite adquirir memoria a través de la red o en un equipo en vivo.

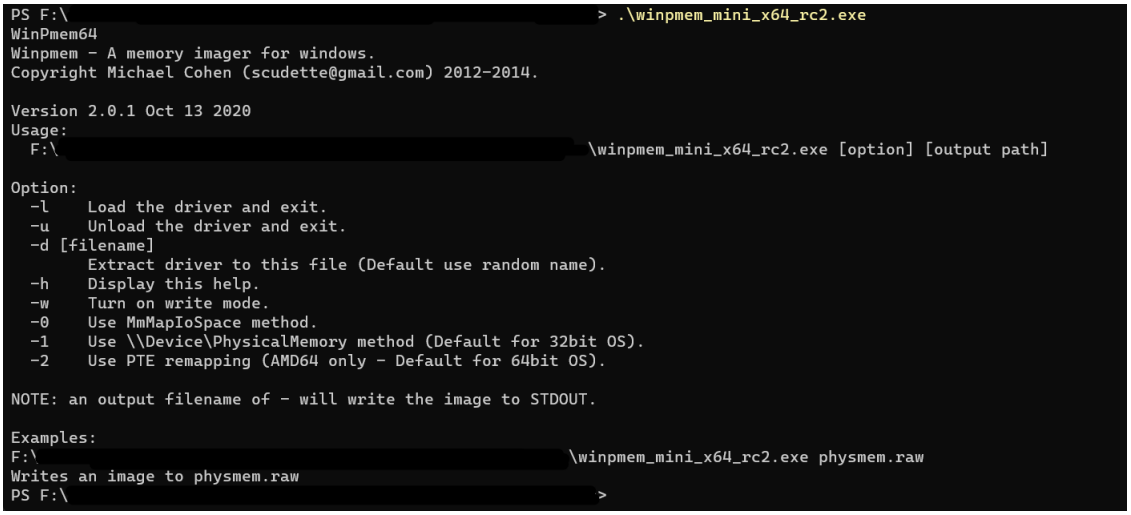


Figura 38. Pantalla principal de WinPMem

Para capturar la memoria simplemente se lanza el ejecutable en una terminal indicando un nombre para el fichero de salida, y el programa comenzará el volcado de la memoria en el archivo de la ruta de salida seleccionada. Al terminar, se podrá acceder al archivo creado y comprobar que efectivamente, vuelca todo el contenido de la memoria, 16,4 GB de tamaño total.

Figura 39. Tamaño captura de la memoria en WinPMem

5.3.2. Características principales

En este apartado se analizarán las características principales de la herramienta WinPMem.

5.3.2.1. Velocidad de obtención del volcado de datos.

Nota: en las pruebas de velocidad con esta herramienta no se ha utilizado la aplicación de cronómetro propia de Windows 10, ya que la herramienta indica el tiempo del sistema al iniciar la captura y al terminarla, por lo que se puede calcular la duración de manera más precisa que utilizando un programa externo.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **2 minutos y 44 segundos**, sin margen de error al estar calculado directamente por la propia aplicación.

Figura 40. Primera captura con WinPMem

En la **segunda prueba**, el tiempo total ha sido de **2 minutos y 44 segundos**, el mismo que en la primera prueba, y sin margen de error al estar calculado directamente por la propia aplicación.

Figura 41. Segunda captura con WinPMem

En la **tercera prueba**, el tiempo ha sido de **2 minutos y 40 segundos**, lo que la sitúa en mejor posición que las dos primeras pruebas.

Figura 42. Tercera captura con WinPMem

La media de **duración de captura en HDD** para la **herramienta WinPMem** es de **2 minutos y 43 segundos**, sin margen de error y redondeado hacia arriba (42,66 segundos).

Por último, en la **prueba con SSD**, el tiempo ha sido de **20 segundos**, sin margen de error. La diferencia con la captura en HDD es de 2 minutos y 23 segundos.

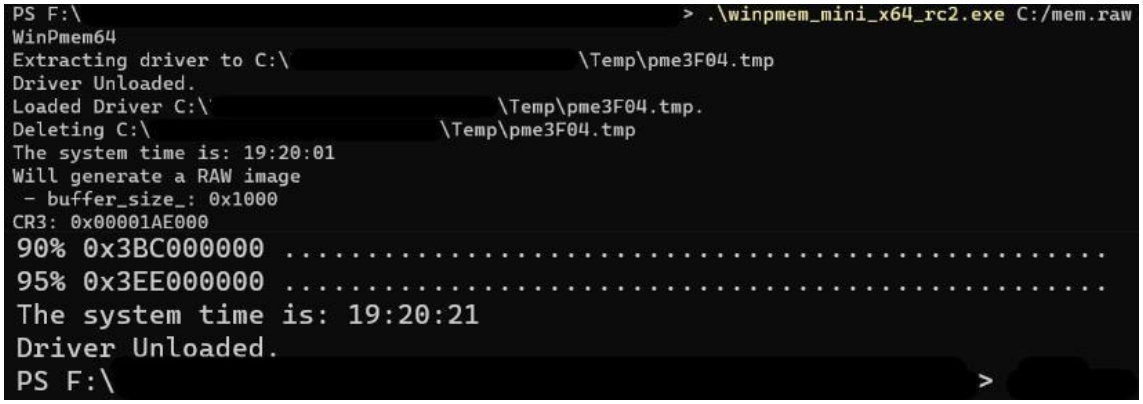


Figura 43. Captura con SSD en WinPMem

5.3.2.2. Impacto en el rendimiento del equipo

Durante la captura, el rendimiento del equipo apenas se ha visto afectado por la herramienta. En el administrador de tareas, el programa WinPMem utiliza durante las tres pruebas de HDD de esta adquisición, una media de 1% de tiempo de CPU y 47 MB de memoria RAM. El factor que más se ha visto afectado es el rendimiento del disco duro, el cual se mantiene constante en una media de unos 102 MB/s, una velocidad bastante buena para un disco duro corriente.

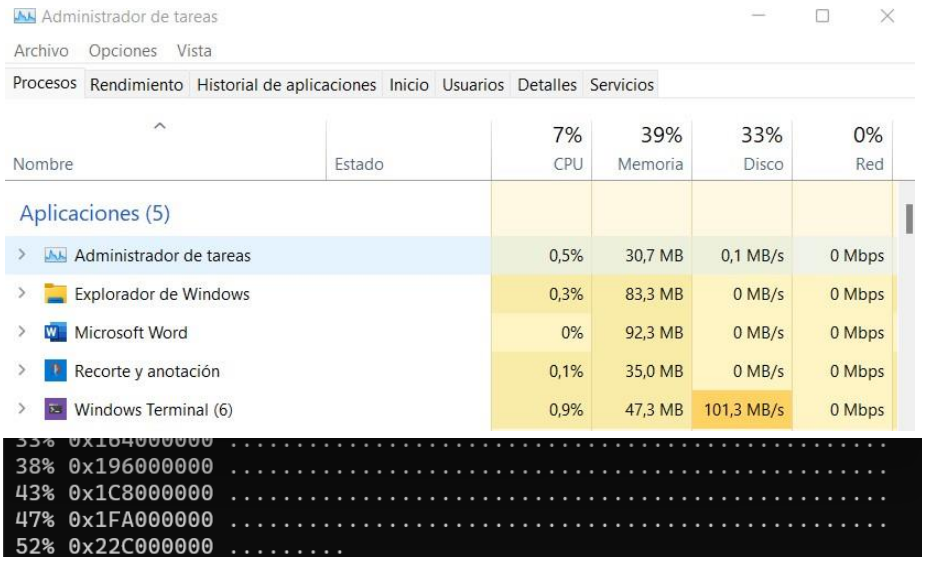


Figura 44. Impacto en el rendimiento HDD en WinPMem

En cuanto al impacto en la prueba con SSD, se puede apreciar un incremento en el uso de CPU, con una subida del 1% en el caso de HDD hasta un 4,3% para esta prueba con SSD, lo que indica un mayor aprovechamiento de la CPU. El consumo de memoria apenas se ve afectado y se mantiene en 48 MB, un MB más que en la prueba con HDD. Como era de esperar, el impacto en el disco es el que se ve más influenciado por el uso del SSD, alcanzando una media constante de 570 MB/s, una velocidad muy elevada que consigue volcar 16 GB de memoria RAM en apenas 20 segundos.

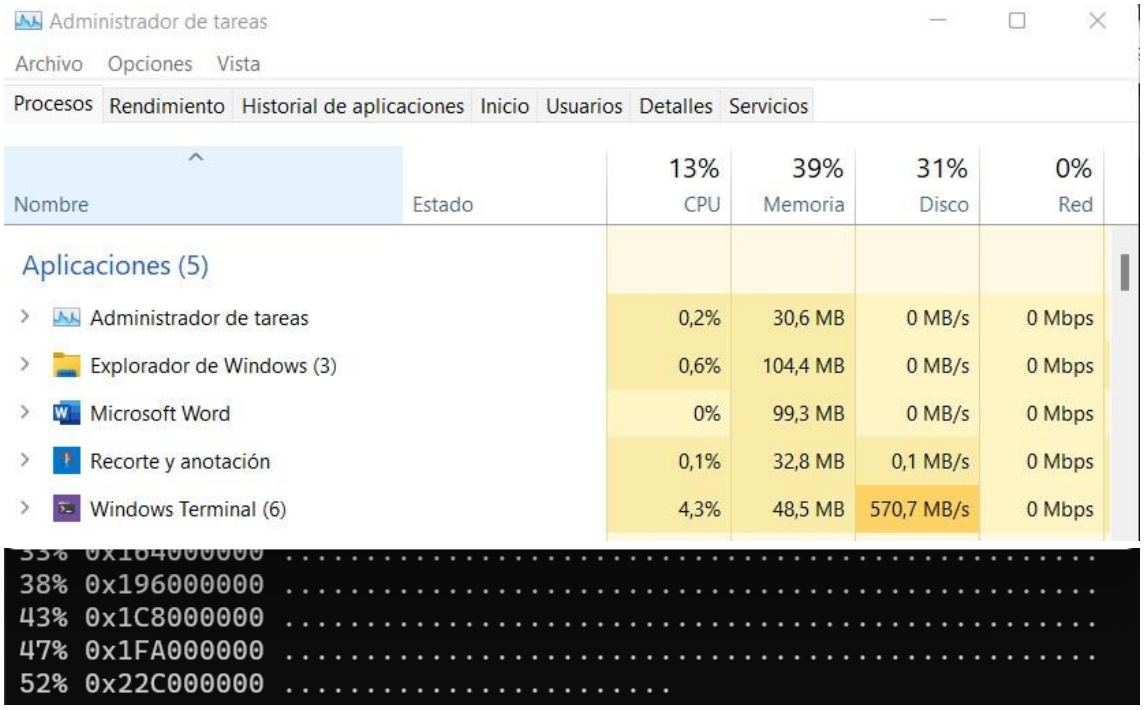


Figura 45. Impacto en el rendimiento SSD en WinPMem

5.3.2.3. Opciones adicionales de captura

WinPMem dispone de varias opciones adicionales de captura, todas consultables en la pantalla principal de la herramienta. Aparte de las distintas opciones de tratamiento de drivers, que no son opciones sobre la captura en sí, sino más bien condiciones de captura, la herramienta presenta tres métodos de adquisición de memoria. Una opción que se puede habilitar es la de utilizar el método MmMapIoSpace para obtener la memoria, un método que, a partir de un rango físico de memoria, devuelve la dirección virtual de memoria correspondiente a ese rango. Este método es útil para drivers de dispositivos que necesitan utilizar buffers de entrada/salida durante largo tiempo [20].

```
Option:
  -l    Load the driver and exit.
  -u    Unload the driver and exit.
  -d [filename]
        Extract driver to this file (Default use random name).
  -h    Display this help.
  -w    Turn on write mode.
  -0    Use MmMapIoSpace method.
  -1    Use \\Device\PhysicalMemory method (Default for 32bit OS).
  -2    Use PTE remapping (AMD64 only - Default for 64bit OS).
```

Figura 46. Opciones adicionales de captura de WinPMem

Otro método consiste en obtener la memoria de la ruta \\Device\PhysicalMemory, método por defecto en sistemas de 32 bits. Por último, se puede obtener la memoria mediante PTE remapping (Page Table Entry), un método que consiste en ignorar las restricciones del sistema operativo sobre la caché de memoria [21].

5.3.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta la herramienta WinPMem.

5.3.3.1. Portabilidad

WinPMem es una herramienta que solamente necesita de un ejecutable para funcionar, por lo que la portabilidad está asegurada. Un ejecutable de poco tamaño es fácilmente portable en cualquier unidad extraíble, incluso una de poca capacidad. Además, la herramienta no necesita instalación para funcionar, simplemente se necesita iniciar el ejecutable desde una terminal, por lo que se puede realizar la captura desde la propia unidad extraíble, aunque como ya se ha comprobado en el caso de FTK Imager, la captura sea muy lenta.

5.3.3.2. Tamaño total de la herramienta

Al tratarse de un ejecutable, el tamaño de la herramienta es muy pequeño, solamente 515 KB. Al no necesitar instalación en el equipo, este es el espacio máximo que ocupará en cualquier equipo o unidad extraíble.

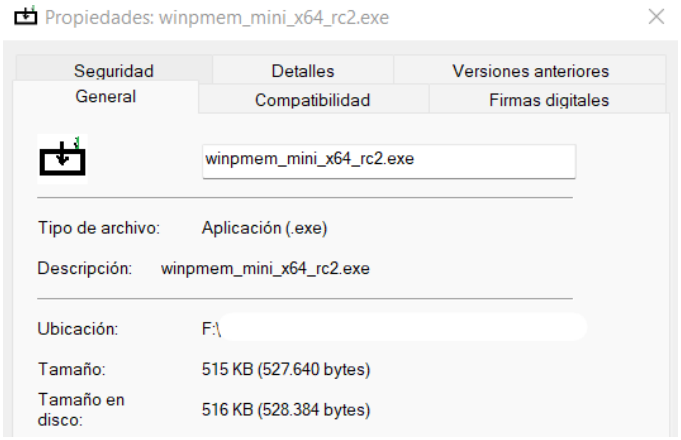


Figura 47. Tamaño total de WinPMem

5.3.3.3. Tipo de licencia

Como ya se ha detallado anteriormente, WinPMem es una herramienta Open Source con licencia Apache 2.0, lo que permite acceder al código fuente y poder utilizarla y compartirla libremente. El proyecto se encuentra ahora en un repositorio en Github fácilmente accesible, de forma que se puede elegir compilar el código por cuenta propia, aunque también se puede descargar directamente el ejecutable compilado con todas las librerías necesarias incluidas.

5.3.3.4. Funcionalidades adicionales

WinPMem no dispone de funcionalidades adicionales a la captura de memoria que no se hayan mencionado con anterioridad. Es una herramienta cuyo único propósito es el volcado de datos de la memoria, disponiendo de varios modos para ello.

5.3.3.5. Experiencia de usuario

Al tratarse de una herramienta ejecutada por línea de comandos, su accesibilidad se ve claramente reducida, siendo necesario tener algo de conocimiento de terminal para utilizarla. Además, las opciones de captura que presenta son bastante avanzadas, y requieren de conocimiento técnico sobre memoria RAM para utilizarlas plenamente. No obstante, para iniciar una captura, solamente se necesita invocar a la herramienta en el prompt del terminal e indicar un nombre con el que guardar la captura para que se obtenga un volcado de la memoria, sin más complicaciones ni necesidad de introducir parámetros extra en la llamada a la herramienta. Por último, la información que se muestra por pantalla al llamar al ejecutable sin nombre de archivo destino es bastante clara y está bien organizada, sin tener que hacer scroll para leer el contenido de la ayuda. Si bien es cierto, la ayuda podía contar con un apartado en el que se explicara un poco en qué consisten los modos de captura, pues ni siquiera en el repositorio oficial se explica en qué se basan los métodos y pueden resultar muy impactantes a primera vista si no se tiene el contexto necesario.

5.3.4. Conclusiones

En conclusión, WinPMem es una herramienta simple y rápida (una captura de 16 GB de memoria en 20 segundos es muy poco tiempo) para obtener un volcado de datos de la memoria RAM, aunque no dispone de ninguna opción adicional y puede llegar a abrumar con sus modos de captura avanzados. Sin embargo da lo que promete, que es una herramienta muy ligera y portable con la que capturar memoria de forma rápida y eficaz de distintos modos.

Ventajas: Velocidad de captura, modos de captura.

Desventajas: Modos difíciles de comprender, sin opciones adicionales.

Valoración final: 9/10

5.4. Belkasoft Live RAM Capturer

La siguiente herramienta que se va a analizar se trata de Belkasoft Live RAM Capturer, en su versión 1.0 lanzada en noviembre de 2020.

5.4.1. Descripción

Belkasoft Live RAM Capturer es una herramienta de interfaz gráfica comercial desarrollada por Belkasoft. Es una herramienta ligera que permite el volcado de la memoria volátil de un sistema incluso cuando este está protegido por sistemas anti volcado, ya que trabaja en el espacio del kernel del sistema y no en espacio de usuario como la mayoría de herramientas [22]. Para conseguir esto, Belkasoft Live RAM Capturer utiliza controladores específicos del sistema operativo para poder acceder al espacio del kernel. Además, con esta herramienta, la memoria que está protegida porque está siendo utilizada por un proceso se puede analizar y capturar de manera íntegra, a diferencia de otras herramientas que operan solamente en espacio de usuario.

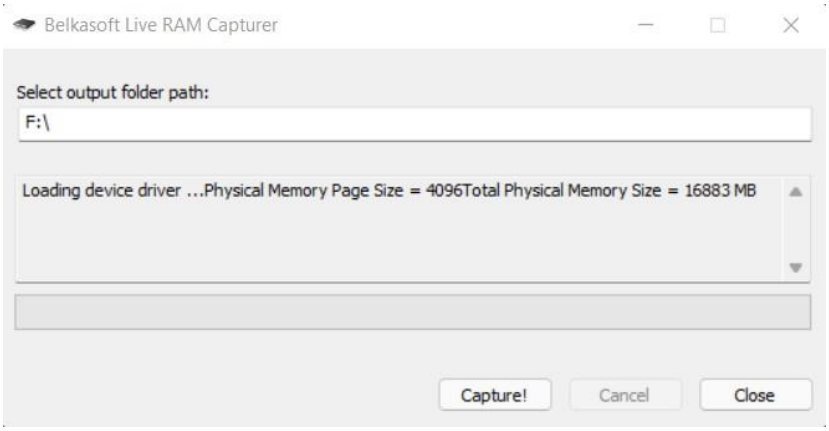


Figura 48. Pantalla principal de Belkasoft Live RAM Capturer

Para capturar la memoria simplemente se inicia el programa y se indica la ruta de salida, y la herramienta comenzará el volcado de la memoria en la ruta de salida seleccionada, con un nombre de archivo correspondiente a la fecha de captura. Al terminar, se podrá acceder al archivo creado y comprobar que efectivamente, vuelca todo el contenido de la memoria, 16,4 GB de tamaño total, tamaño que se indica también al terminar la captura en la propia herramienta.

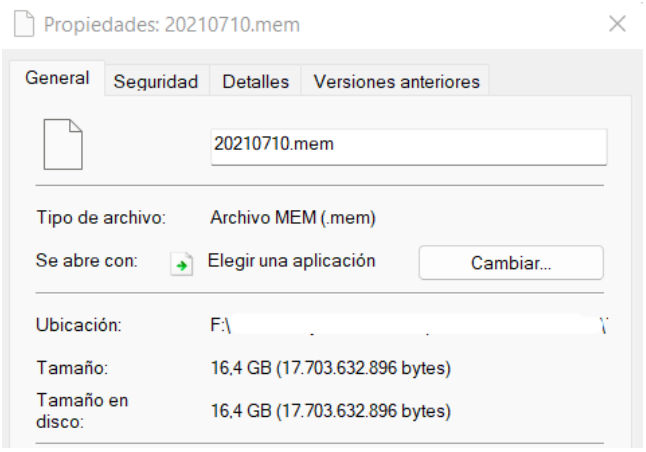


Figura 49. Tamaño captura de la memoria en Belkasoft Live RAM Capturer

5.4.2. Características principales

En este apartado se analizarán las características principales de Belkasoft Live RAM Capturer.

5.4.2.1. Velocidad de obtención del volcado de datos.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **3 minutos y 10 segundos**, con un margen de error de 1 segundo, entre que se inicia y se para el contador y se cambia de ventana.

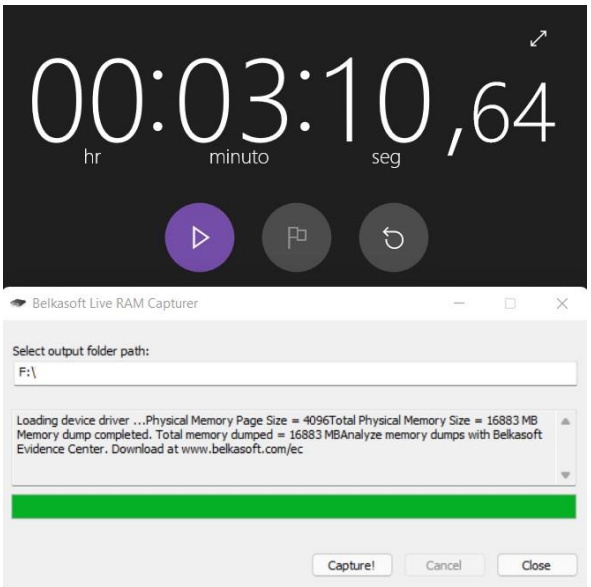


Figura 50. Primera captura con Belkasoft Live RAM Capturer

En la **segunda prueba**, el tiempo total ha sido de **2 minutos y 57 segundos**, con el mismo margen de error de 1 segundo que en la prueba anterior.

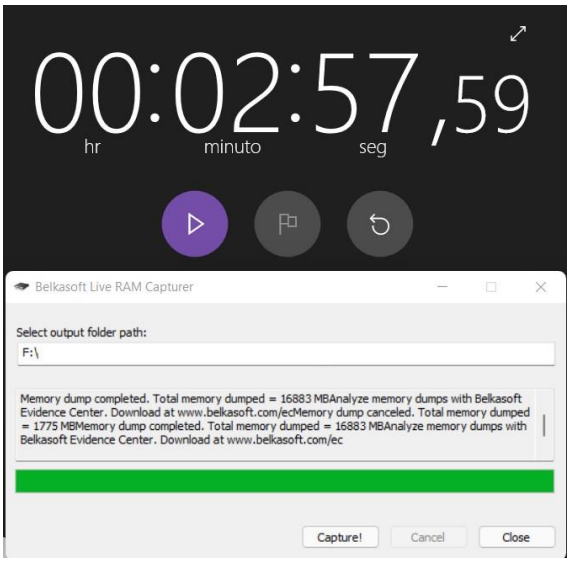


Figura 51. Segunda captura con Belkasoft Live RAM Capturer

En la **tercera prueba**, el tiempo ha sido de **3 minutos y 8 segundos**, lo que la sitúa entre las dos primeras pruebas, con un margen de error de 1 segundo.

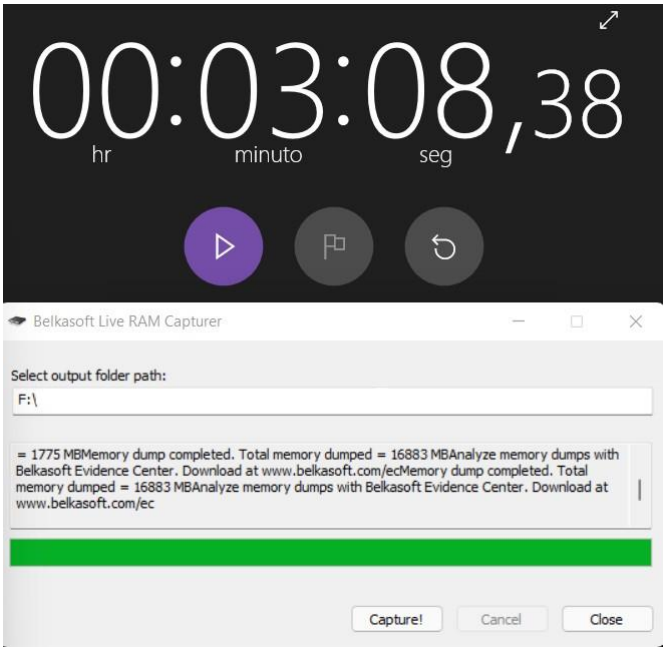


Figura 52. Tercera captura con Belkasoft Live RAM Capturer

La media de **duración de captura en HDD** para la **herramienta Belkasoft Live RAM Capturer** es de **3 minutos y 5 segundos** con margen de error de 1 segundo.

Por último, en la **prueba con SSD**, el tiempo ha sido de **24 segundos**, con margen de error de 1 segundo. La diferencia con la captura en HDD es de 2 minutos y 39 segundos.

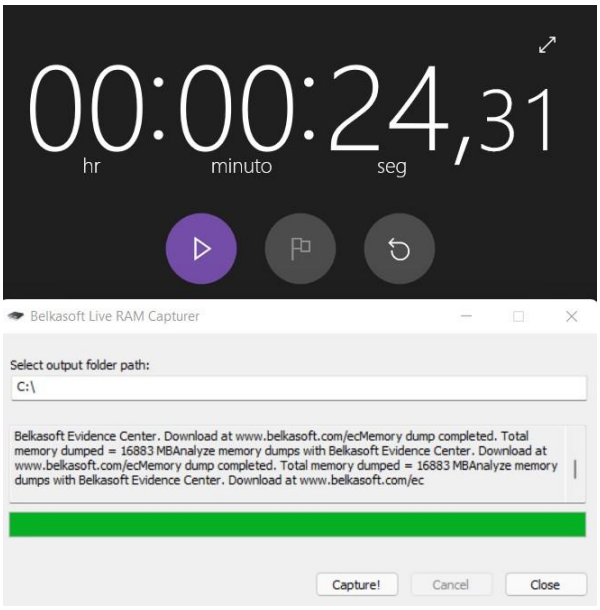


Figura 53. Captura con SSD en Belkasoft Live RAM Capturer

5.4.2.2. Impacto en el rendimiento del equipo

Durante la captura, el rendimiento del equipo apenas se ha visto afectado por la herramienta. En el administrador de tareas, Belkasoft Live RAM Capturer utiliza durante las tres pruebas de HDD de esta adquisición, una media de 1% de tiempo de CPU y solamente 1,6 MB de memoria RAM, algo bastante interesante y poco habitual. El factor que más se ha visto afectado es el rendimiento del disco duro, el cual se mantiene constante en unos valores entre 90 y 100 MB/s, una velocidad bastante adecuada para un disco duro corriente.

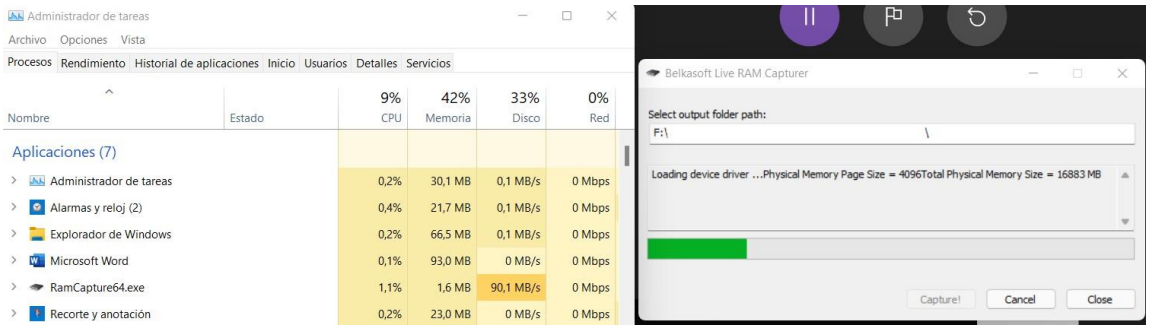


Figura 54. Impacto en el rendimiento HDD en Belkasoft Live RAM Capturer

En cuanto al impacto en la prueba con SSD, se puede apreciar un incremento en el uso de CPU, con una subida del 1% en el caso de HDD hasta un 7% para esta prueba con SSD, lo que indica un mayor aprovechamiento de la CPU. El consumo de memoria apenas se ve afectado y se mantiene en un increíble 1 MB de uso. Como era de esperar, el impacto en el disco es el que se ve más influenciado por el uso del SSD, alcanzando una media constante de 700 MB/s, una velocidad muy elevada que consigue volcar 16 GB de memoria RAM en apenas 24 segundos.

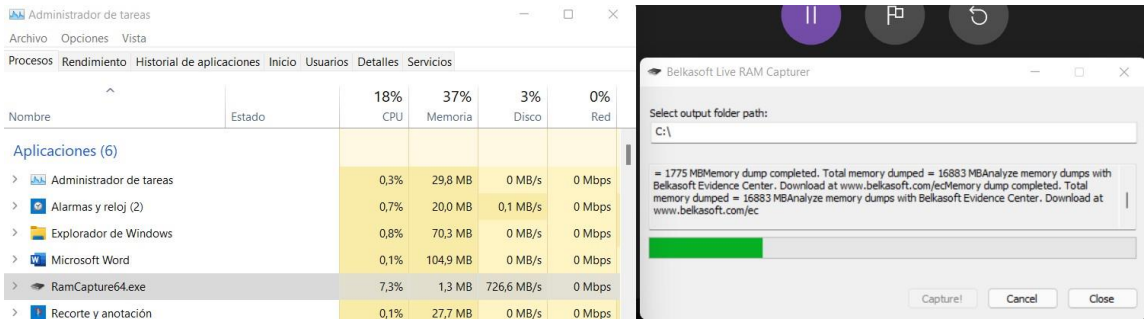


Figura 55. Impacto en el rendimiento SSD en Belkasoft Live RAM Capturer

5.4.2.3. Opciones adicionales de captura

Belkasoft Live RAM Capturer no dispone de ninguna opción adicional de captura, simplemente permite la adquisición de memoria de una forma, indicando la ruta de destino, ni siquiera se puede cambiar el formato del archivo salida ni el nombre del mismo.

5.4.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta Belkasoft Live RAM Capturer.

5.4.3.1. Portabilidad

Al tratarse de un ejecutable que no requiere instalación, la portabilidad de la herramienta es máxima, ya que se puede descargar en un dispositivo extraíble USB y utilizarla para extraer la memoria de cualquier equipo desde allí. El único inconveniente, como ya se ha comentado en la prueba desde USB con FTK Imager, es que la captura es extremadamente lenta, ya que está limitada por el ancho de banda de transferencia del USB, que mejorará en el caso de ser USB 3.0.

5.4.3.2. Tamaño total de la herramienta

Al tratarse de un ejecutable, el tamaño de la herramienta es muy pequeño, solamente 57,1 KB, ocupando 60 KB en disco.

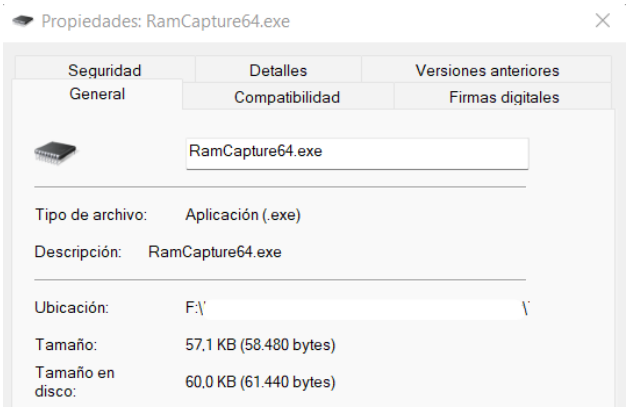


Figura 56. Tamaño del ejecutable de Belkasoft Live RAM Capturer

Sin embargo, este solamente es el tamaño del ejecutable, pero necesita otros 3 archivos dll con las librerías necesarias para funcionar correctamente. Esto incrementa significativamente el tamaño total de la herramienta hasta llegar a los 1,52 MB.

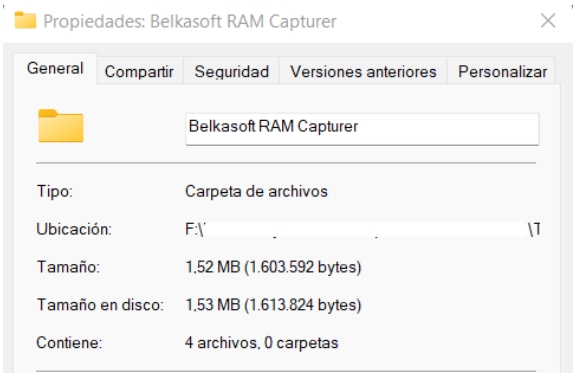


Figura 57. Tamaño total de la herramienta Belkasoft Live RAM Capturer

5.4.3.3. Tipo de licencia

Como ya se ha detallado anteriormente, Belkasoft Live RAM Capturer es una herramienta gratuita con licencia comercial por la empresa Belkasoft. Para solicitar una copia de la herramienta, se debe solicitar en su página oficial, indicando primero un correo electrónico organizativo, y después rellenando un formulario similar al de la herramienta FTK Imager, en el que se debe rellenar el nombre, apellidos, teléfono, puesto de trabajo y país. Una vez completada la encuesta, se enviará un correo con el enlace directo de descarga de la herramienta.

5.4.3.4. Funcionalidades adicionales

Belkasoft Live RAM Capturer no dispone de ninguna funcionalidad adicional, al igual que no disponía de opciones adicionales a la captura, simplemente se utiliza para volcar rápidamente la memoria RAM de un sistema.

5.4.3.5. Experiencia de usuario

Esta herramienta no dispone de guía de usuario alguna sobre cómo utilizar la herramienta, pero tampoco es necesaria, ya que simplemente es indicar una ruta y pulsar en capturar. Al ser una herramienta con interfaz gráfica, es más accesible que una que funciona por línea de comandos, además de la facilidad de uso general de la herramienta, simplemente se lanza el ejecutable y se captura, sin opciones ni modos complejos que requieren amplia formación en temas de memoria volátil.

5.4.4. Conclusiones

En conclusión, Belkasoft Live RAM Capturer es una herramienta simple y bastante rápida para obtener un volcado de datos de la memoria RAM, pero que no dispone de ninguna opción adicional de captura ni de otras opciones adicionales a la captura, lo que resta en funcionalidad. Sin embargo, es una herramienta muy ligera y portable que no requiere instalación, con una interfaz simple y fácil de utilizar por cualquier usuario sin importar su nivel de conocimientos ni experiencia en memoria volátil.

Ventajas: Simpleza, fácil de utilizar.

Desventajas: Variedad de opciones.

Valoración final: 8/10

5.5. Winen (EnCase)

La siguiente herramienta que se va a analizar se trata de Winen, un ejecutable disponible junto con el software forense EnCase, en su versión 6.9.16 lanzada en junio de 2008.

5.5.1. Descripción

Winen es una herramienta de línea de comandos comercial disponible junto con el software EnCase Forensic, desarrollados por Guidance Software, ahora llamada OpenText. Se trata de un ejecutable que funciona de manera independiente al software forense, es más, no se puede ejecutar desde el mismo, debe lanzarse en solitario para capturar la memoria. Para poder utilizar Winen, se debe acceder a la ruta de instalación de EnCase y lanzar el ejecutable winen.exe o winen64.exe, según la compatibilidad con el equipo en el que se capturará la memoria, desde una terminal con permisos de administrador. Winen permite la captura de memoria en formato E01, el mismo que se podía indicar en la herramienta FTK Imager, para que después se pueda analizar de forma íntegra con EnCase.

```
PS C:\Program Files (x86)\EnCase6> .\winen64.exe -h
Usage: [Options]
-p <EvidencePath>: Evidence File Path
-m <EvidenceName>: Evidence Name (Max Size:50)
-c <CaseNumber>: Case Number (Max Size:64)
-e <Examiner>: Examiner Name (Max Size:64)
-r <EvidenceNumber>: Evidence Number (Max Size:64)
-d <Compress>: Compression level (0=None, 1=Fast, 2=Best) (Default: 0) (min:0 max:2)
-a <AlternatePath>: A semicolon delimited list of Alternate paths
-n <Notes>: Notes (Max Size:32768)
-s <MaxFileSize>: Maximum file size in MB (Default: 640) (min:1 max:10485760)
-g <Granularity>: Error granularity (Sectors) (Default: 1) (min:1 max:1024)
-b <BlockSize>: Block size (Sectors) (Default: 64) (min:1 max:1024)
-f <File>: Path to configuration file
-t: Turns off hashing the evidence file (default: true)
-1: Turns on SHA1 hashing of the evidence file (default: false)
-h: This help message
PS C:\Program Files (x86)\EnCase6>
```

Figura 58. Pantalla principal de Winen

Para capturar la memoria se inicia el programa y se indican las opciones obligatorias que muestra por pantalla, como la ruta de salida, el nombre del archivo, o el número y nombre del caso forense asociado a la captura, y la herramienta comenzará el volcado de la memoria. Al terminar, se podrá acceder a los archivos E0X creados (se crearán tantos archivos como tamaño de segmento se haya configurado) y comprobar que efectivamente, entre todos, se vuelca todo el contenido de la memoria, 16,4 GB de tamaño total.

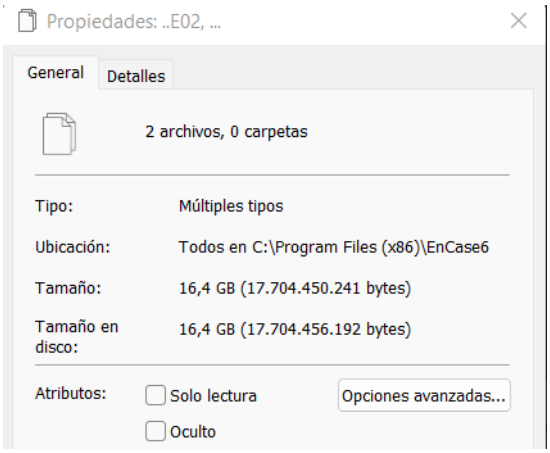


Figura 59. Tamaño captura de la memoria en Winen

5.5.2. Características principales

En este apartado se analizarán las características principales de Winen.

5.5.2.1. Velocidad de obtención del volcado de datos.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **3 minutos y 21 segundos**, con un margen de error de 1 segundo, entre que se inicia y se para el contador y se cambia de ventana.

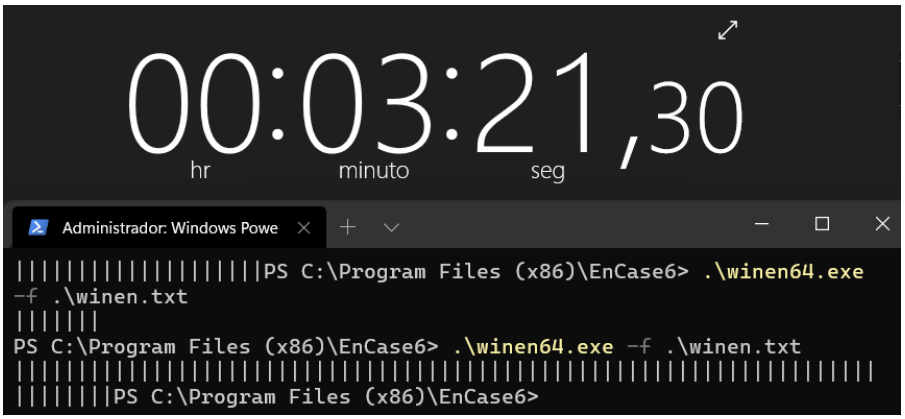


Figura 60. Primera captura con Winen

En la **segunda prueba**, el tiempo total ha sido de **2 minutos y 47 segundos**, con el mismo margen de error de 1 segundo que en la prueba anterior.

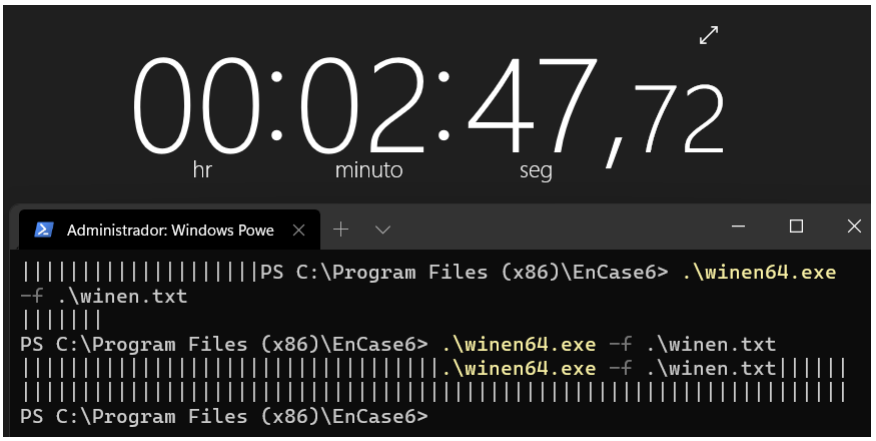


Figura 61. Segunda captura con Winen

En la **tercera prueba**, el tiempo ha sido de **2 minutos y 49 segundos**, lo que la sitúa entre las dos primeras pruebas, con un margen de error de 1 segundo.

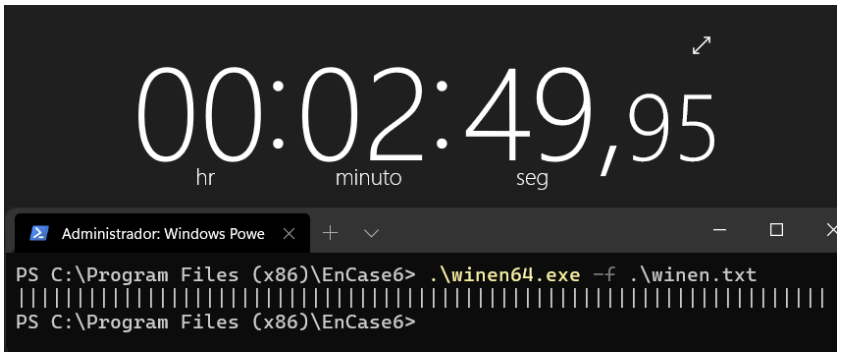


Figura 62. Tercera captura con Winen

La media de **duración de captura en HDD** para la **herramienta Winen** es de **2 minutos y 58 segundos** con margen de error de 1 segundo.

Por último, en la **prueba con SSD**, el tiempo ha sido de **1 minuto y 16 segundos**, con margen de error de 1 segundo. La diferencia con la captura en HDD es de 1 minutos y 42 segundos.

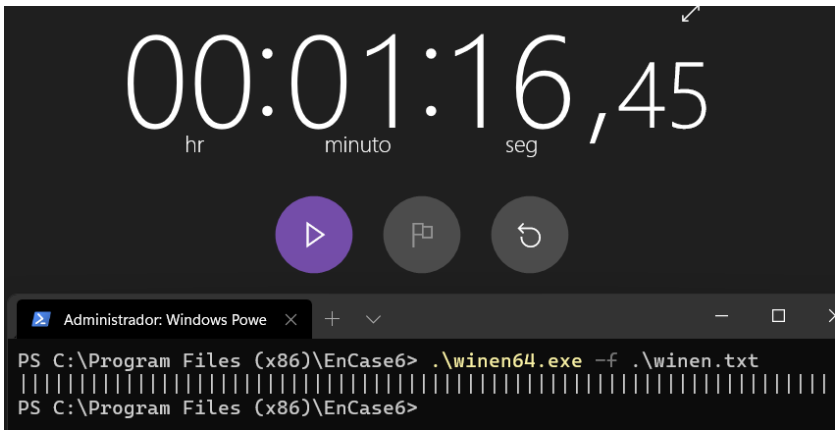


Figura 63. Captura con SSD en Winen

5.5.2.2. Impacto en el rendimiento del equipo

Durante la captura, el rendimiento del equipo apenas se ha visto afectado por la herramienta. En el administrador de tareas, Winen utiliza durante las tres pruebas de HDD de esta adquisición, una media de 3% de uso de CPU y 58,3 MB de memoria RAM. El factor que más se ha visto afectado es el rendimiento del disco duro, el cual se mantiene constante en 77 MB/s, una velocidad similar a la de otras herramientas.

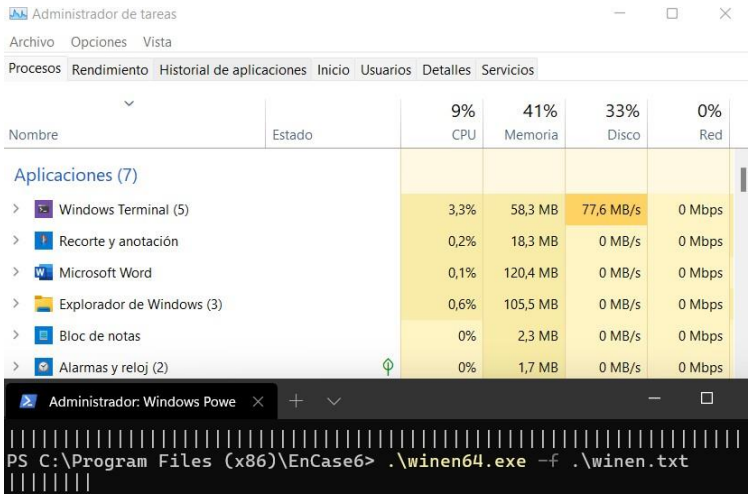


Figura 64. Impacto en el rendimiento HDD en Winen

En cuanto al impacto en la prueba con SSD, se puede apreciar un incremento en el uso de CPU, con un 8% de utilización, lo que indica un mayor aprovechamiento de la CPU. El consumo de memoria apenas se ve afectado y se mantiene en 58,4 MB. Sorprendentemente, el impacto en el disco SSD no es tan grande como en pruebas con otras herramientas, en las que el impacto en el disco es mayor, hasta llegar en algunos casos a los 700 MB/s. En el caso de Winen, la velocidad se mantiene en unos 230 MB/s, lo que demuestra el tiempo extra en la captura de la memoria y que no se está aprovechando el disco SSD en su totalidad.

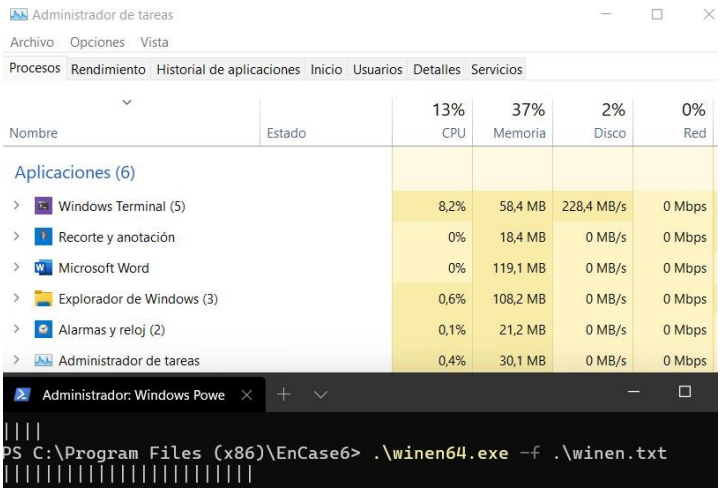


Figura 65. Impacto en el rendimiento SSD en Winen

5.5.2.3. Opciones adicionales de captura

Winen dispone de algunas opciones adicionales de captura, como la posibilidad de asignar un número a la evidencia obtenida y un nombre al investigador que la ha extraído, de forma que se

pueda identificar más fácilmente la cadena de custodia de una evidencia forense. También es posible establecer un tamaño máximo de archivo, lo que divide la captura total en archivos del mismo tamaño, útil para poder trabajar con la información de manera más sencilla. Por último, se puede establecer un nivel de compresión para la captura, pudiendo elegir entre 3 opciones: ninguna compresión (opción predeterminada), compresión rápida o mejor compresión. Se ha probado con la compresión rápida, y el resultado de la captura en disco HDD es el siguiente.

Figura 66. Prueba de captura con compresión rápida en Winen

La duración de la captura aumenta desde los 3 minutos aproximados sin compresión hasta los 6 minutos y 17 segundos, más del doble de tiempo. Sin embargo, el archivo resultado con la evidencia ha visto reducido su tamaño en un 50%, ahora ocupa unos 8 GB.

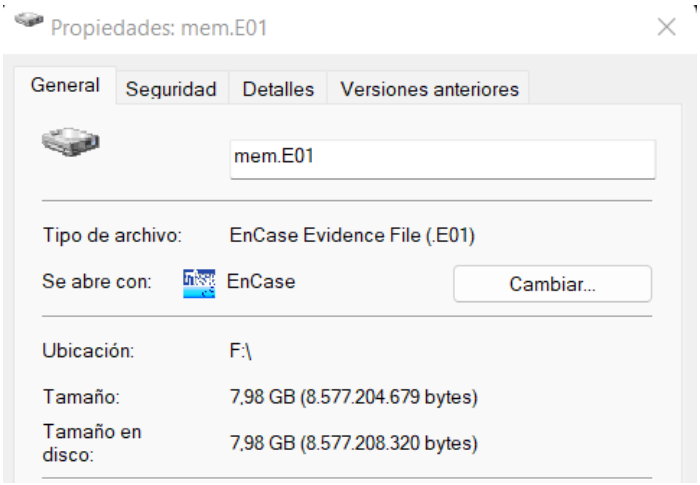


Figura 67. Tamaño de la captura de memoria con compresión rápida en Winen

Por otro lado, un inconveniente que presenta Winen es que el único formato de archivo que acepta es E01, el propio de EnCase, lo que dificulta la compatibilidad con otros programas de análisis de memoria RAM.

5.5.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta la herramienta Winen.

5.5.3.1. Portabilidad

Al igual que en el caso de la herramienta WinPMem, al tratarse de un ejecutable que no requiere instalación, la portabilidad de Winen es máxima, ya que se puede descargar en un dispositivo extraíble USB y utilizarla para extraer la memoria de cualquier equipo desde allí. El único

inconveniente, como ya se ha comentado en la prueba desde USB con FTK Imager, es que la captura es extremadamente lenta, ya que está limitada por el ancho de banda de transferencia del USB, que mejorará en el caso de ser USB 3.0.

5.5.3.2. Tamaño total de la herramienta

Al tratarse de un ejecutable, el tamaño de la herramienta es pequeño, un total de 408 KB de espacio en disco. Además, este es el tamaño total de la herramienta, pues no necesita otros archivos ni instalación para funcionar.

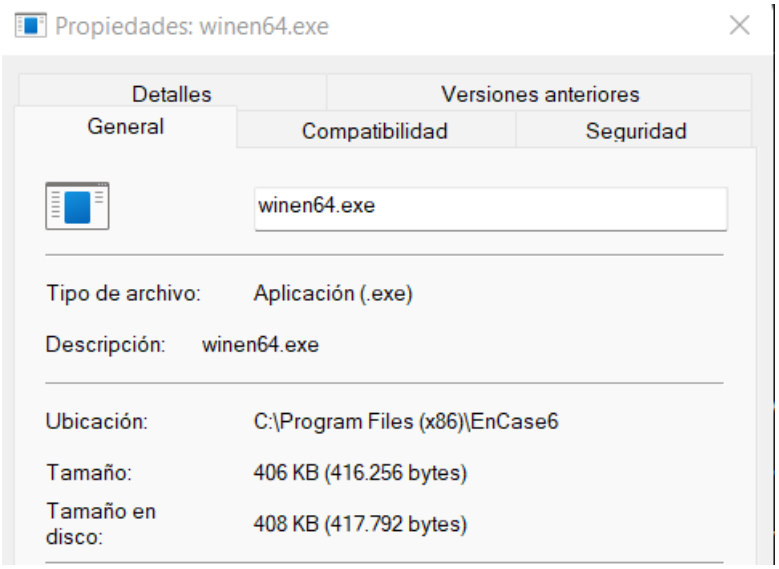


Figura 68. Tamaño del ejecutable de Winen

5.5.3.3. Tipo de licencia

Como ya se ha detallado anteriormente, Winen es una herramienta comercial empaquetada en el software forense EnCase. No existe versión gratuita, para obtener la herramienta se debe solicitar acceso a la suite completa en la página oficial de OpenText. Actualmente, existen versiones antiguas en Internet de EnCase, antes de que Guidance Software, la empresa original desarrolladora de la suite fuera adquirida por OpenText, por lo que se puede obtener de manera gratuita, pero las últimas versiones son de pago sin opción de prueba gratuita.

5.5.3.4. Funcionalidades adicionales

Winen dispone de alguna funcionalidad adicional, como la posibilidad de calcular el hash de la evidencia tras obtenerla, lo que resulta muy útil en investigaciones forenses para asegurar la cadena de custodia y la integridad del archivo. Otra opción más compleja es la de establecer la granularidad en sectores de la memoria, así como el tamaño de bloque, en el que se indican los sectores por bloque. Otras opciones adicionales son la posibilidad de enviar la evidencia adquirida a otras rutas del equipo y poder escribir notas extra en la evidencia, que se podrán leer al analizar el archivo de datos.

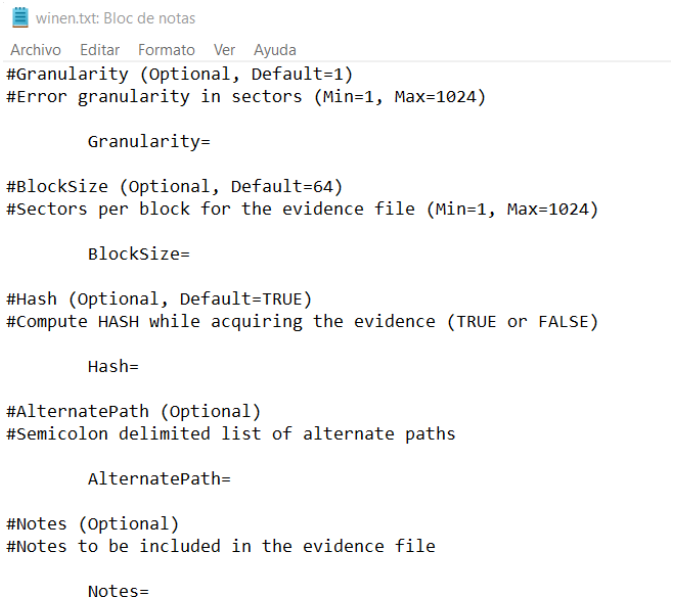


Figura 69. Funcionalidades adicionales de Winen

5.5.3.5. *Experiencia de usuario*

Esta herramienta no dispone de guía de usuario alguna sobre cómo utilizar la herramienta, pero si se introduce el parámetro -h se mostrará una ventana con todas las opciones de la herramienta.Sin embargo, se trata de una herramienta de línea de comandos, lo que la hace más compleja queotra que funcione mediante interfaz gráfica. Además, al contrario que en el caso de WinPMem, en el que se podía capturar la memoria simplemente especificando un nombre de archivo destino,en este caso se deben introducir otros parámetros adicionales, lo que la convierten en una herramienta más compleja. No obstante, si simplemente se ejecuta sin introducir ningún parámetro, Winen pedirá al usuario los datos mínimos necesarios para ejecutarse, por lo que no es necesario conocer los parámetros ni los valores que se pueden introducir. Por último, aunque no disponga de guía de usuario, EnCase proporciona un archivo de texto con las opciones disponibles en la herramienta Winen, por lo que se puede rellenar ese archivo y luego pasarlo como parámetro de entrada a la herramienta, facilitando aún más el uso.

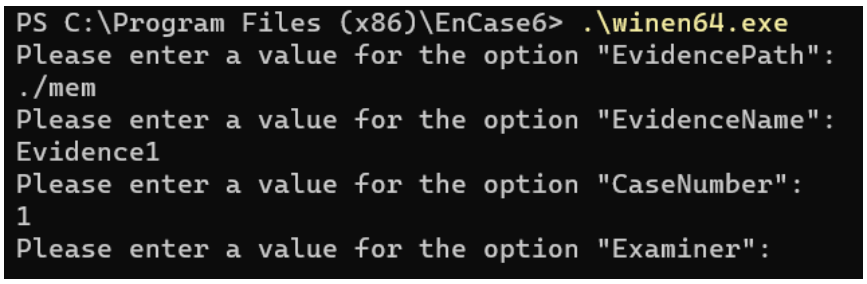


Figura 70. Ayuda al usuario durante la captura sin parámetros de Winen

5.5.4. Conclusiones

En conclusión, Winen es una herramienta simple de utilizar para obtener un volcado de datos de la memoria RAM, disponiendo además de alguna opción interesante desde el punto de vista del análisis forense, lo que hace que sea una alternativa a tener en cuenta si se desea trabajar con evidencias y se quiere tener un control sobre las mismas, gracias en parte a su numeración de

casos y evidencias y a la posibilidad de calcular el hash del archivo al obtener el volcado de datos. Asimismo, es una herramienta muy ligera y portable que no requiere instalación, pero su tipo de licencia y las restricciones que presenta para poder utilizarla (requiere licencia de EnCase, que no es barata) disminuyen su difusión y posibilidades de uso.

Ventajas: Características forenses, portabilidad.

Desventajas: Tipo de licencia.

Valoración final: 7,2/10

5.6. Win64dd (Moonsols Windows Memory Toolkit)

La siguiente herramienta que se va a analizar se trata de Moonsols Windows Memory Toolkit Community Edition, en concreto el módulo win64dd.exe, en su versión 1.3.1 lanzada en octubre de 2010.

5.6.1. Descripción

Win64dd es un módulo perteneciente a la herramienta comercial Moonsols Windows Memory Toolkit (MWMT), desarrollada por la start-up MoonSols. Se trata de un ejecutable que funciona por línea de comandos y permite la captura de memoria del sistema de forma directa, volcando todo el contenido de la memoria en bruto, pudiendo trabajar además con volcados de errores y de hibernación de Microsoft o con volcados de máquinas virtuales de VMWare [23]. Este módulo tiene su correspondencia en versión de 32 bits, llamado win32dd, pero en este análisis se utilizará la versión de 64 bits al ser compatible con el equipo de pruebas detallado. Además de las opciones de captura mencionadas previamente, win64dd permite crear el hash de la captura obtenida, utilizar varios modos de obtención del volcado de datos o enviar la captura de la memoria a un servidor remoto mediante SMB.

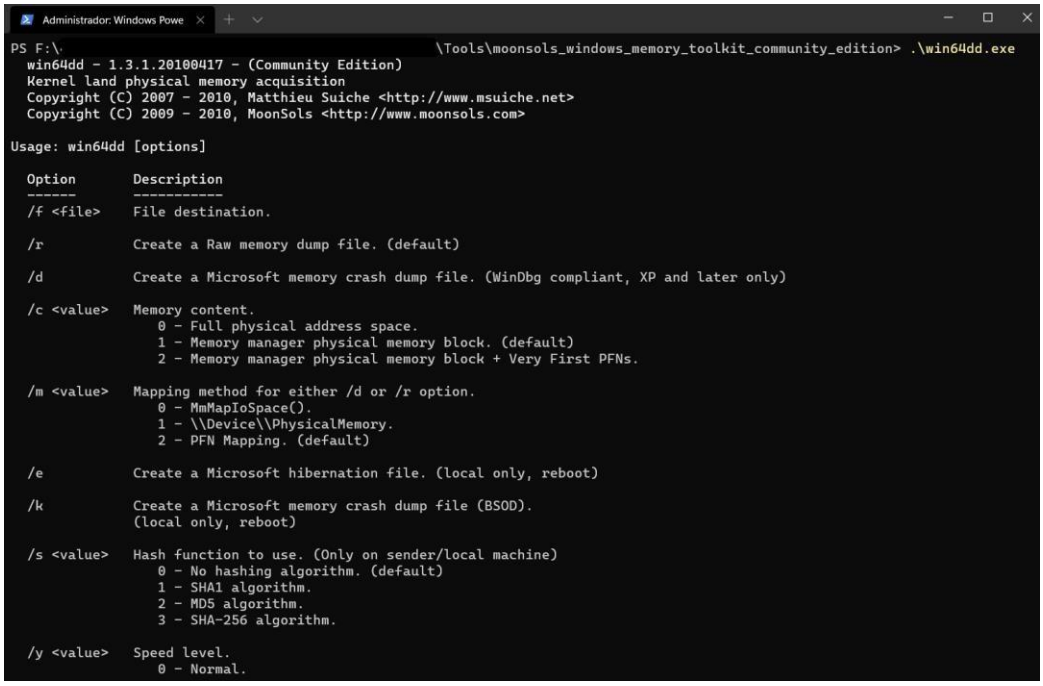


Figura 71. Pantalla principal del módulo win64dd.exe de MWMT

Para realizar una captura completa de la memoria se inicia el programa y se indica el parámetro */f ./mem* para asignar un nombre y un destino a la evidencia. Al terminar, se podrá acceder al archivo de memoria creado y comprobar que efectivamente, se vuelca todo el contenido de la memoria, 16,4 GB de tamaño total.

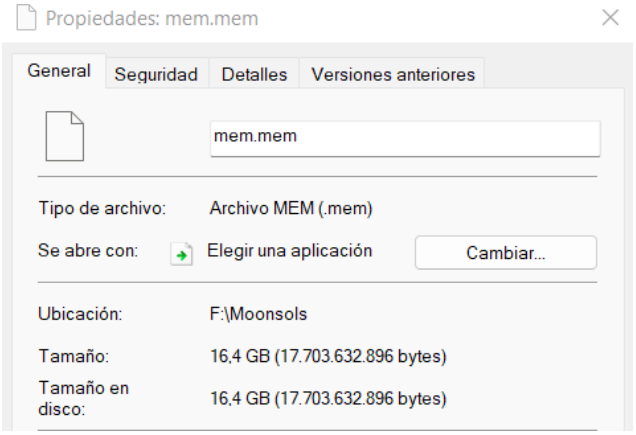


Figura 72. Tamaño captura de la memoria en win64dd

5.6.2. Características principales

En este apartado se analizarán las características principales de win64dd.

5.6.2.1. Velocidad de obtención del volcado de datos.

Nota: en las pruebas de velocidad con esta herramienta no se ha utilizado la aplicación de cronómetro propia de Windows 10, ya que la herramienta indica el tiempo del sistema al iniciar la captura y al terminarla, por lo que se puede calcular la duración de manera más precisa que utilizando un programa externo.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **3 minutos y 58 segundos**, sin margen de error, ya que el tiempo es calculado por la propia aplicación.

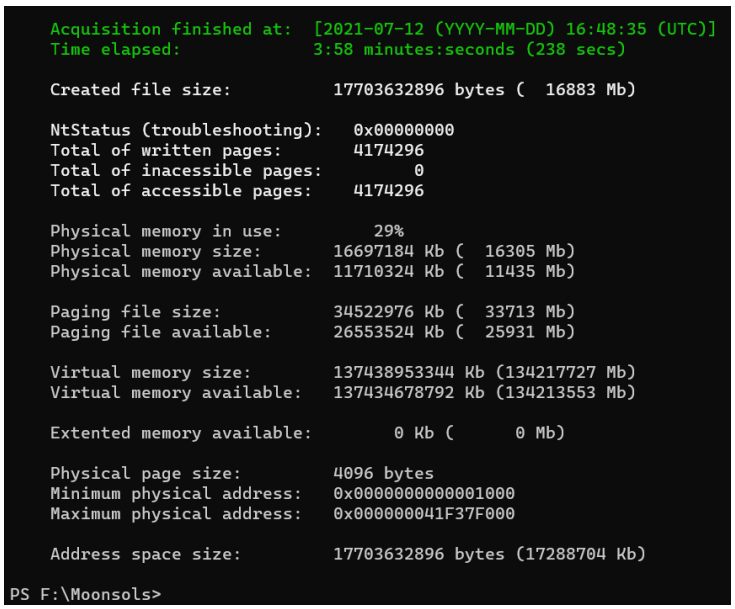


Figura 73. Primera captura con win64dd

En la **segunda prueba**, el tiempo total ha sido de **3 minutos y 41 segundos**, sin margen de error.

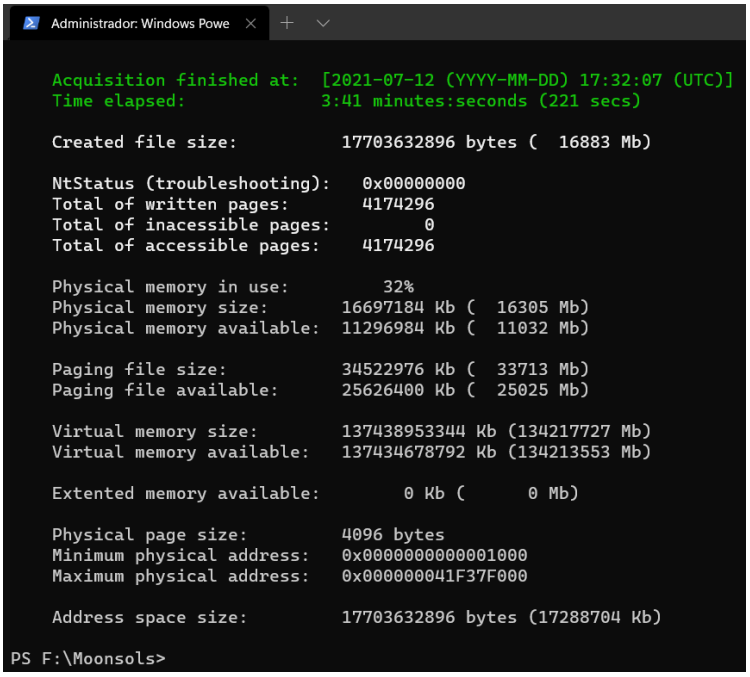


Figura 74. Segunda captura con win64dd

En la **tercera prueba**, el tiempo ha sido de **3 minutos y 35 segundos**, sin margen de error, lo que la convierte en la mejor prueba hasta ahora.

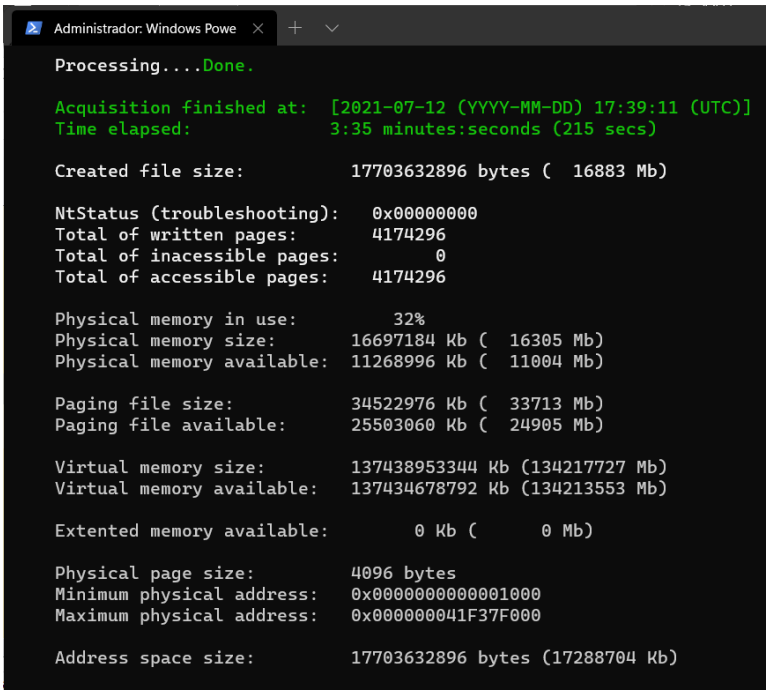


Figura 75. Tercera captura con win64dd

La media de **duración de captura en HDD** para el proceso **win64dd** es de **3 minutos y 44 segundo,** sin margen de error.

Por último, en la **prueba con SSD**, el tiempo ha sido de **16 segundos**, sin margen de error. La diferencia con la captura en HDD es de 3 minutos y 28 segundos.

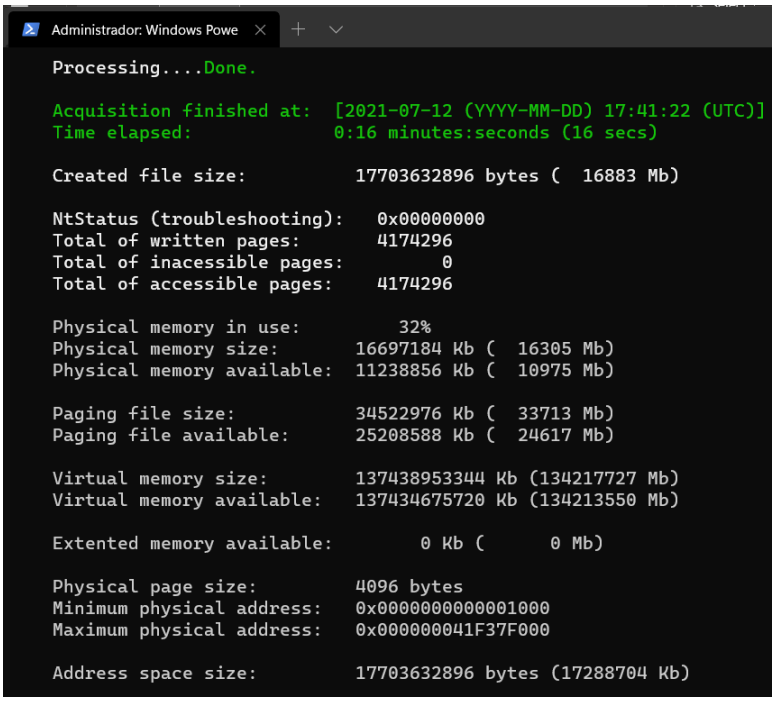


Figura 76. Captura con SSD en win64dd

5.6.2.2. Impacto en el rendimiento del equipo

Durante la captura, el rendimiento del equipo apenas se ha visto afectado por la herramienta. En la prueba con HDD, el uso de CPU se ha mantenido en el 0,1%, mientras que la memoria utilizada por el proceso Windows terminal ha sido de 24 MB. Curiosamente, en el caso de esta herramienta, la ejecución del módulo no entra dentro del proceso general Windows terminal, sino que se crea un proceso de Windows secundario llamado win64dd.exe, que utiliza el disco duro, mientras que el uso de CPU y memoria recae sobre el proceso de la terminal. El uso del disco duro, por su parte, se ha mantenido en 72,5 MB/s, una velocidad similar a la de otras herramientas para un HDD.

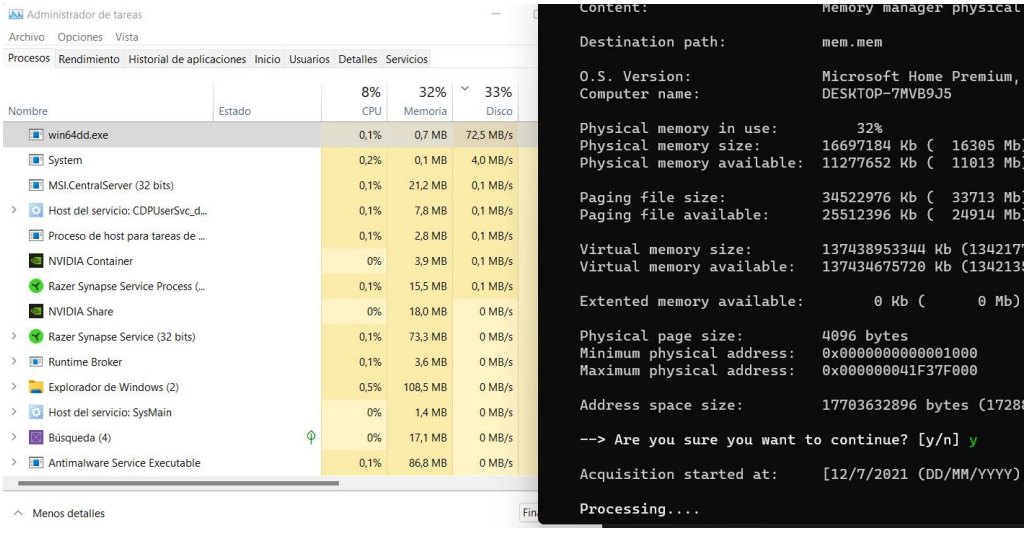


Figura 77. Impacto en el rendimiento HDD en win64dd

En cuanto al impacto en la prueba con SSD, se obtienen los mismos resultados para el uso de memoria, 24MB, pero ahora la CPU ha aumentado su uso hasta llegar a un 1,7% de utilización, lo que indica un mayor aprovechamiento de la CPU. El uso del disco duro, por su parte, se ha mantenido en los 773 MB/s, comenzando en velocidades superiores a los 1000 MB/s, lo cual podría resultar falso si no fuera por el tiempo que tarda en capturar la memoria, solamente 16 segundos.

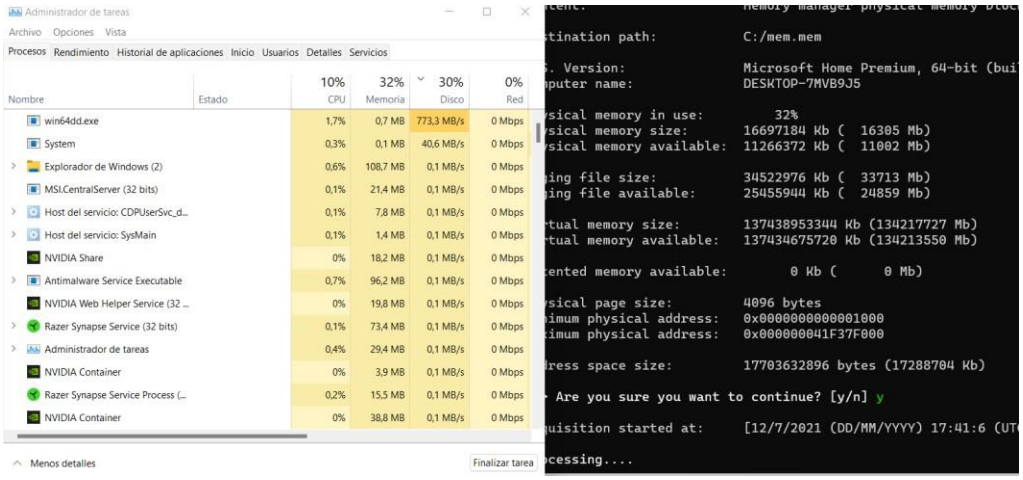


Figura 78. Impacto en el rendimiento SSD en win64dd

5.6.2.3. Opciones adicionales de captura

El proceso win64dd, como ya se ha mencionado, dispone de varias opciones adicionales de captura. Las más importantes son la posibilidad de generar un fichero de volcado de errores de Microsoft, compatible además con la herramienta WinDbg para poder analizar la causa de posibles errores presentes en el equipo de forma sencilla; así como poder generar un fichero de hibernación y un fichero de cuelgue del equipo, la popularmente conocida pantalla azul de la muerte (BSOD), pero requiere reiniciar el equipo.

```
/f <file>    File destination.

/r           Create a Raw memory dump file. (default)

/d           Create a Microsoft memory crash dump file. (WinDbg compliant, XP

/c <value>   Memory content.
                0 - Full physical address space.
                1 - Memory manager physical memory block. (default)
                2 - Memory manager physical memory block + Very First PFNs.

/m <value>   Mapping method for either /d or /r option.
                0 - MmMapIoSpace().
                1 - \\Device\\PhysicalMemory.
                2 - PFN Mapping. (default)

/e           Create a Microsoft hibernation file. (local only, reboot)

/k           Create a Microsoft memory crash dump file (BSOD).
             (local only, reboot)

/s <value>   Hash function to use. (Only on sender/local machine)
                0 - No hashing algorithm. (default)
                1 - SHA1 algorithm.
                2 - MD5 algorithm.
                3 - SHA-256 algorithm.

/y <value>   Speed level.
                0 - Normal.
                1 - Fast.
                2 - Sonic.
                3 - Hyper sonic. (default)
```

Figura 79. Opciones adicionales de captura en win64dd

Otras opciones interesantes son los distintos modos de captura de la memoria, pudiendo elegir todo el espacio físico de la misma, el bloque de memoria presente en el gestor de memoria y ese bloque junto con los primeros PFN (Page Frame Number), que devuelve los primeros valores disponibles para asignar a los archivos del equipo en memoria. Una opción que ya presentaba WinPMem, es la posibilidad de seleccionar el método de mapeado de la memoria, utilizando el método MmMapIoSpace, la ruta \\Device\\PhysicalMemory, o el mapeado por PFN, el usado por defecto si no se indica lo contrario. Por último, se puede asignar una velocidad a la captura, siendo la velocidad más rápida (Hyper Sonic) la seleccionada por defecto.

5.6.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta el módulo win64dd.

5.6.3.1. Portabilidad

Similar a otras herramientas de línea de comandos, al tratarse de un ejecutable que no requiere instalación, la portabilidad de win64dd es máxima, ya que se puede descargar en un dispositivo extraíble USB y utilizar este módulo para extraer la memoria de cualquier equipo desde allí. El único inconveniente, como ya se ha comentado en la prueba desde USB con FTK Imager, es que la captura es extremadamente lenta, ya que está limitada por el ancho de banda de transferencia del USB, que mejorará en el caso de ser USB 3.0.

5.6.3.2. Tamaño total de la herramienta

Al tratarse de un ejecutable, el tamaño de win64dd es pequeño, un total de 108 KB de espacio en disco. Además, este es el tamaño total de la herramienta, pues no necesita otros archivos ni instalación para funcionar.

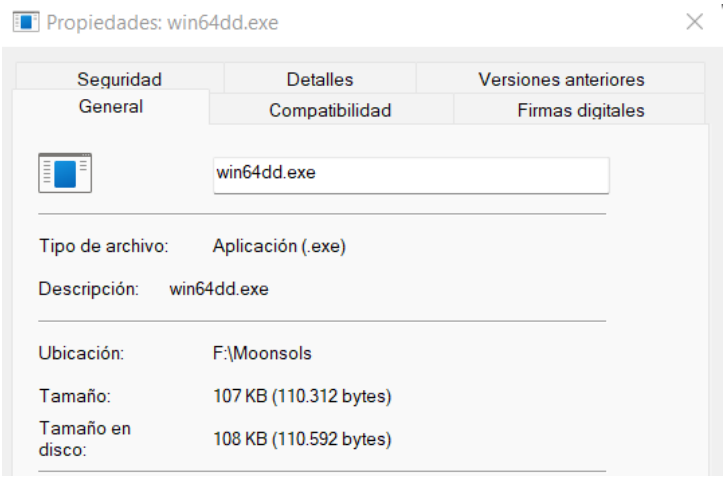


Figura 80. Tamaño del ejecutable de win64dd

5.6.3.3. Tipo de licencia

Como ya se ha detallado anteriormente, win64dd es un módulo perteneciente a una serie de herramientas comerciales empaquetadas en el Moonsols Windows Memory Toolkit. Existen varias versiones diferentes del paquete, desde la versión Community, que es la que se ha analizado y que es gratuita, hasta versiones de pago con soporte directo con Moonsols. Para descargar la Community Edition de este paquete, se debería acceder a la página principal de Moonsols y descargarlo desde allí, pero el botón que debería llevar a la descarga no redirige a ningún sitio web. Por lo tanto, se ha tenido que descargar desde fuera de la página. Aun así, aunque esta

versión es de uso gratuito, está prohibido hacer ingeniería inversa y distribuir la solución, por lo que se trata de una licencia gratuita de uso comercial.

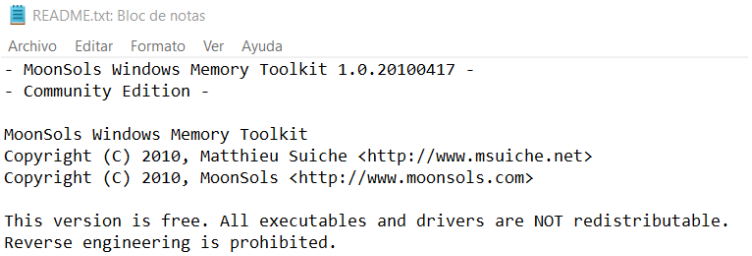


Figura 81. Licencia del módulo win64dd de MWMT

5.6.3.4. Funcionalidades adicionales

Win64dd dispone de alguna funcionalidad adicional, además de las ya mencionadas opciones de captura. Al igual que en el caso de Winen, es posible calcular el hash de la evidencia tras obtenerla, lo que resulta muy útil en investigaciones forenses para asegurar la cadena de custodia y la integridad del archivo. Sin embargo, la gran opción que presenta win64dd es la posibilidad de realizar la captura en un equipo y configurar el envío del volcado a un servidor o a otro equipo mediante SMB. Para que otro equipo reciba el volcado se debe configurar el módulo en modo recepción de datos, para ello se lanza win64dd con el parámetro */l*, que activa el puerto 1337 (por defecto) en modo escucha.

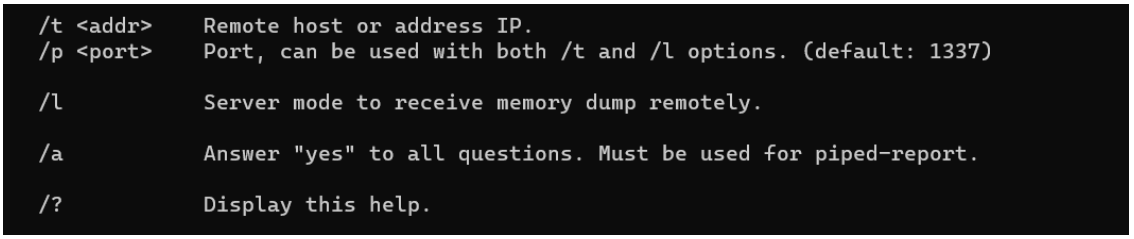


Figura 82. Funcionalidades adicionales de envío de volcado en win64dd

Cabe destacar que, mientras que se ejecuta la herramienta, se muestra una pantalla bastante informativa, con datos técnicos acerca del método de captura seleccionado, los parámetros adicionales introducidos, información del sistema operativo, y mucha información sobre la memoria del sistema, como el espacio físico utilizado actualmente, el tamaño de página o el espacio físico y virtual de direccionamiento.

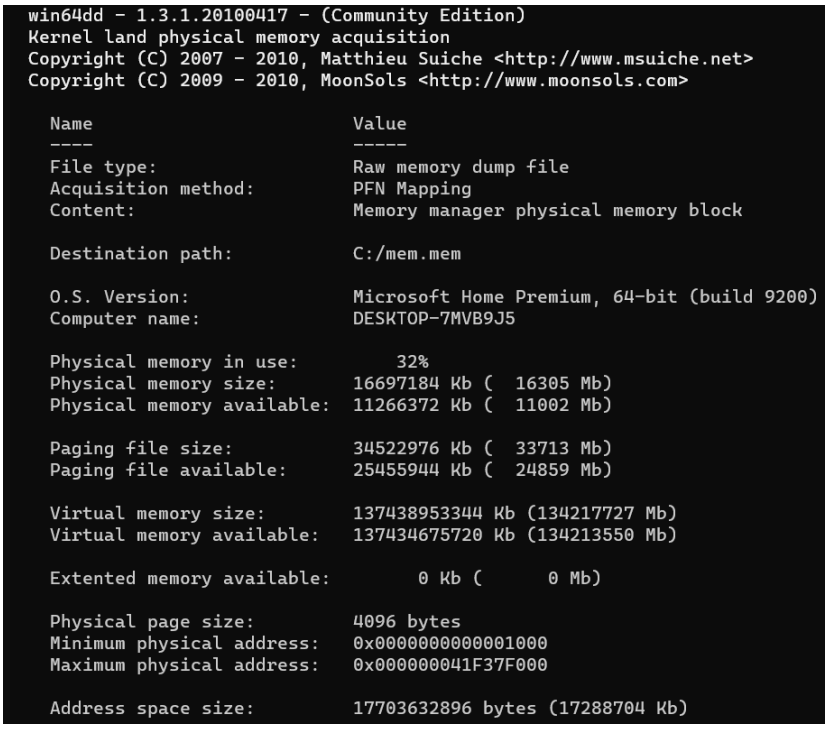


Figura 83. Información técnica adicional en win64dd

5.6.3.5. Experiencia de usuario

Win64dd no dispone de guía de usuario alguna sobre cómo utilizar la herramienta, pero si se lanza el ejecutable sin parámetros se mostrará una ventana con todas las opciones de la herramienta. Sin embargo, se trata de una herramienta de línea de comandos, lo que la hace más compleja que otra que funcione mediante interfaz gráfica. Aun así, la ayuda que se muestra está bien explicada, incluyendo algunos ejemplos de utilización de la herramienta en determinadas situaciones, como por ejemplo para el caso de la configuración de win64dd en modo captura remota.

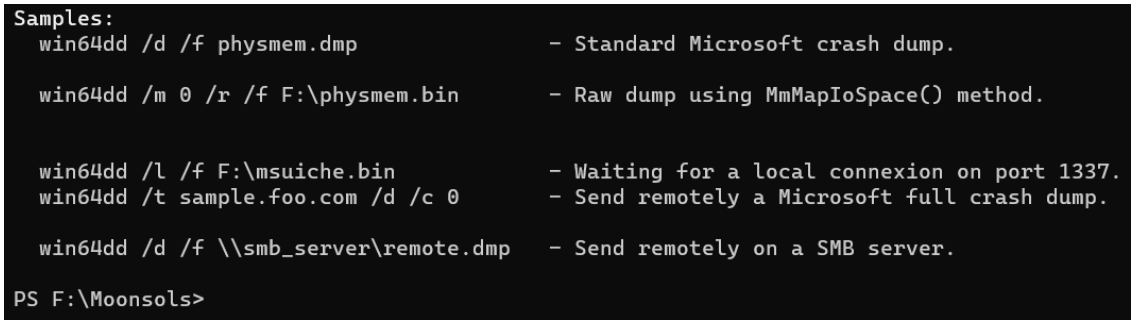


Figura 84. Muestras de ejemplo de uso de comandos de win64dd

5.6.4. Conclusiones

En conclusión, win64dd es una herramienta para obtener un volcado de datos de la memoria RAM que dispone de ciertas características únicas que la diferencian del resto, como la gran cantidad de información técnica que se muestra al iniciar y terminar la captura de memoria, o la posibilidad de enviar el volcado de datos a otro equipo en una red local. Además, también incorpora características ya vistas en otras herramientas como los distintos modos de captura o la opción de calcular el hash del volcado de datos. No obstante, la velocidad de captura en HDD es algo lenta, aunque lo compensa en la captura SSD, y la difusión limitada del paquete, siendo muy difícil de

encontrar en la actualidad, sumado al tipo de licencia que utiliza, hacen que sea poco accesible al público general.

Ventajas: Velocidad captura SSD, múltiples opciones de captura.

Desventajas: Velocidad de captura HDD, herramienta difícil de encontrar.

Valoración final: 8,5/10

5.7. Magnet RAM Capture

La siguiente herramienta que se va a analizar se trata de Magnet RAM Capture, en su versión 1.2.0 de julio de 2019.

5.7.1. Descripción

Magnet RAM Capture es una herramienta gratuita comercial de interfaz gráfica desarrollada por Magnet Forensics que permite la captura de memoria RAM de un equipo con sistema operativo Windows. Magnet RAM Capture tiene una huella de memoria muy pequeña, lo que significa que los investigadores pueden ejecutar la herramienta sin preocuparse de posibles sobreescrituras de datos de la memoria por esta herramienta [24]. Una vez capturada la memoria en un archivo en bruto, se puede utilizar en otra herramienta de análisis de volcado de datos como Magnet AXIOM, o cualquier otra herramienta open source como Volatility.

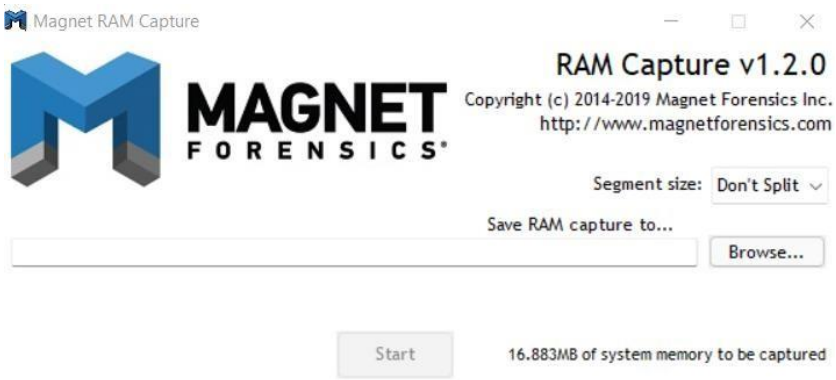


Figura 85. Pantalla principal de Magnet RAM Capture

Para realizar una captura completa de la memoria con Magnet RAM Capture, primero se inicia el programa, se aceptan los términos y condiciones y se indica un nombre y un destino a la evidencia. Al terminar, se podrá acceder al archivo de memoria creado y comprobar que efectivamente, se vuelca todo el contenido de la memoria, 16,4 GB de tamaño total.

Figura 86. Tamaño captura de la memoria en Magnet RAM Capture

5.7.2. Características principales

En este apartado se analizarán las características principales de Magnet RAM Capture.

5.7.2.1. Velocidad de obtención del volcado de datos.

Nota: en estas pruebas se ha comprobado la velocidad de captura utilizando el modo de segmentación de la herramienta, con la esperanza de agilizar la captura, pero el resultado es el mismo con segmentación o sin ella.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **7 minutos y 16 segundos**, con un margen de error de 1 segundo, entre que se cambia la ventana para iniciar y parar el contador.

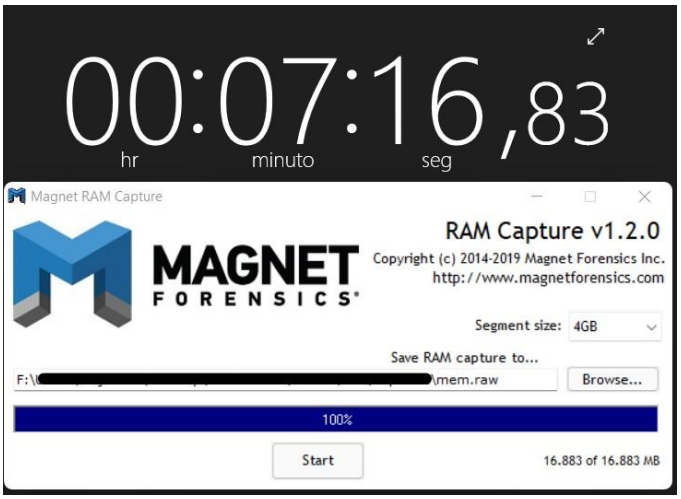


Figura 87. Primera captura con Magnet RAM Capture

En la **segunda prueba**, el tiempo total ha sido de **7 minutos y 7 segundos**, con un margen de error de 1 segundo.

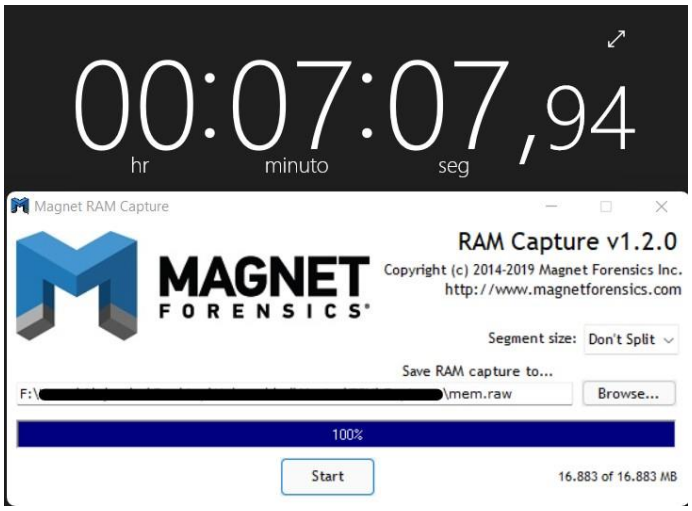


Figura 88. Segunda captura con Magnet RAM Capture

En la **tercera prueba**, el tiempo ha sido de **7 minutos**, con margen de error de 1 segundo, lo que la convierte en la mejor prueba hasta ahora.

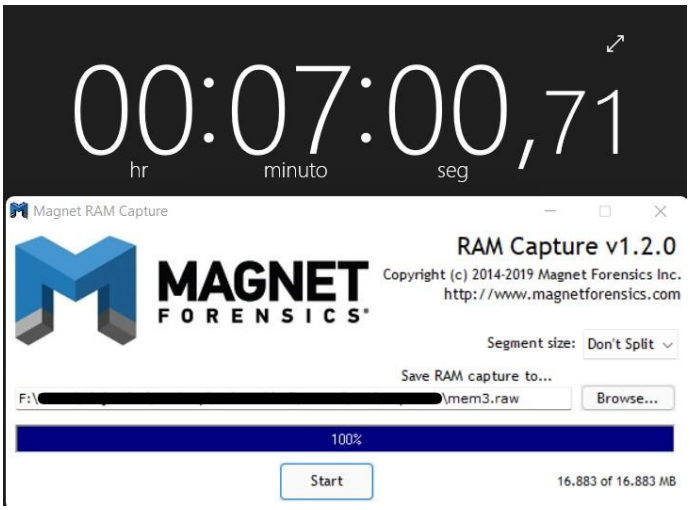


Figura 89. Tercera captura con Magnet RAM Capture

La media de **duración de captura en HDD** para el proceso **win64dd** es de **7 minutos y 7 segundos,** con un margen de error de 1 segundo.

Por último, en la **prueba con SSD**, el tiempo ha sido de **49 segundos**, con margen de error de 1 segundo. La diferencia con la captura en HDD es de 6 minutos y 18 segundos.

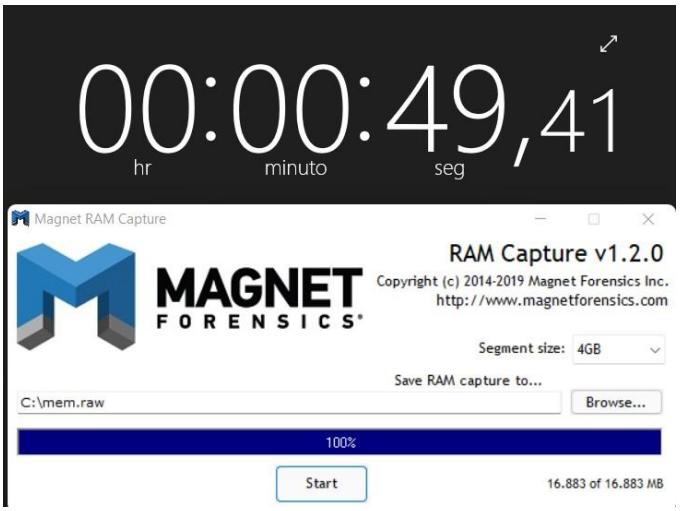


Figura 90. Captura con SSD en Magnet RAM Capture

Una vez realizadas las pruebas, destaca la lentitud de la captura con esta herramienta comparada con las otras analizadas. En el administrador de tareas, se puede observar que el proceso Magnet RAM Capture está en modo de funcionamiento de 32 bits, así que puede ser ese el motivo de la lentitud de la captura, ya que el resto de herramientas se han probado en su versión de 64 bits.

5.7.2.2. Impacto en el rendimiento del equipo

Durante la captura, el rendimiento del equipo apenas se ha visto afectado por la herramienta. En la prueba con HDD, el uso de CPU se ha mantenido en 0,7%, mientras que la memoria ha utilizado 8 MB. Por otro lado, el uso del disco duro se ha mantenido en valores alrededor de los 47 MB/s, una velocidad muy baja para un disco duro HDD, de ahí la larga duración de la captura, 7 minutos. Además, como ya se ha mencionado, modificar el tamaño del segmento del archivo no altera este resultado.

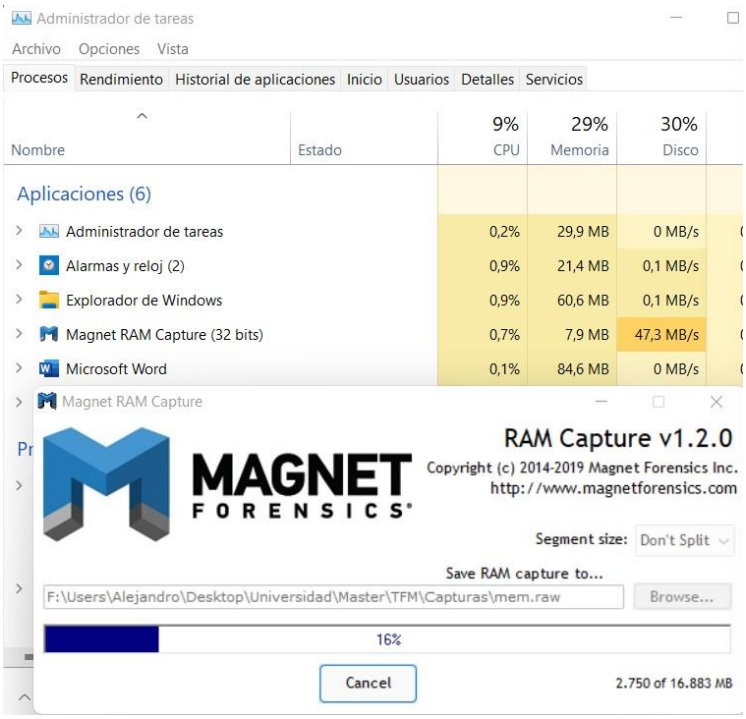


Figura 91. Impacto en el rendimiento HDD en Magnet RAM Capture

En cuanto al impacto en la prueba con SSD, comparando los datos con la captura en HDD, el uso de CPU ha aumentado hasta llegar a un 5,8% de utilización, lo que indica un mayor aprovechamiento de este recurso, mientras que la memoria ha aumentado ligeramente hasta los 13 MB. El uso del disco duro, por su parte, ha alcanzado valores medios de 265 MB/s, número muy bajos si los comparamos con otras herramientas analizadas.

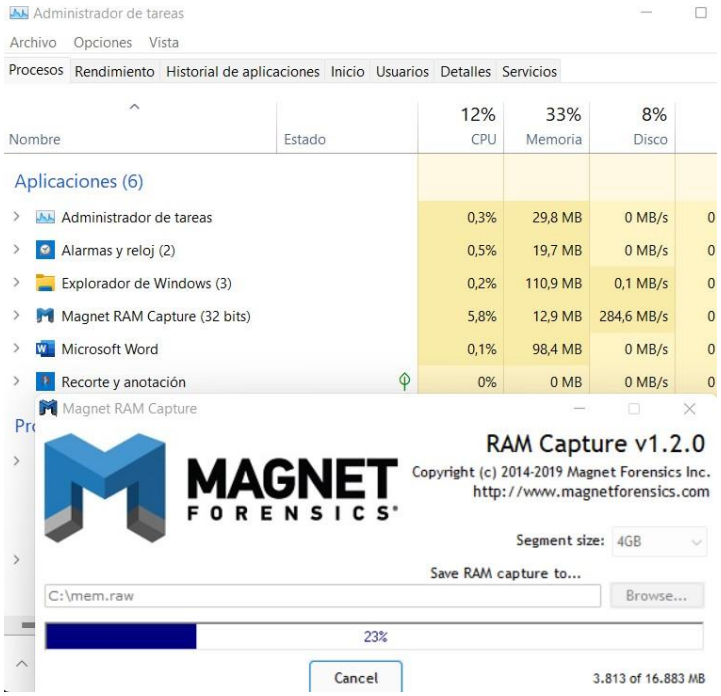


Figura 92. Impacto en el rendimiento SSD en Magnet RAM Capture

La conclusión que se puede obtener de este apartado es que la herramienta no aprovecha al máximo los recursos del equipo, siendo la más lenta de todas las analizadas con diferencia. Es posible que esto se deba a que la versión que se ejecuta es de 32 bits, ya que la descarga que suministra la página no dispone de opción para seleccionar otra versión, es un ejecutable único.

5.7.2.3. Opciones adicionales de captura

Magnet RAM Capture dispone de una sola opción adicional de captura, la posibilidad de segmentar la captura en archivos de igual tamaño, pudiendo elegir tamaños de 500 MB, 1 GB, 2 GB y 4 GB. Esta opción es muy útil en el caso de que la memoria a extraer sea demasiado grande, por ejemplo tamaños mayores a 16 GB, en los que mover y analizar un solo archivo se pueda hacer pesado.

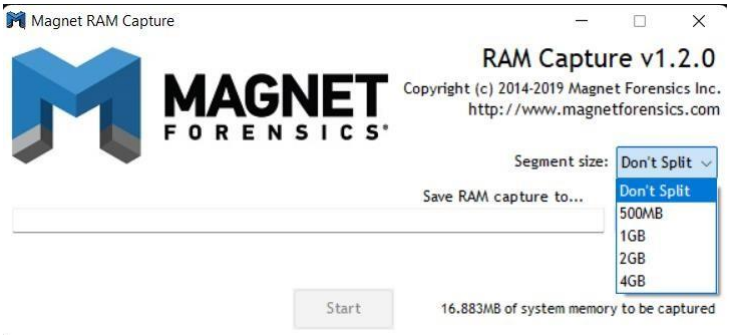


Figura 93. Opciones adicionales de captura en Magnet RAM Capture

5.7.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta Magnet RAM Capture.

5.7.3.1. Portabilidad

Aunque se trate de una herramienta con interfaz gráfica, la portabilidad es máxima, pues simplemente se necesita el ejecutable para poder capturar la memoria de un equipo. Como ya se ha mencionado en otras herramientas, es posible insertar el ejecutable en un dispositivo de almacenamiento externo y capturar la memoria del equipo desde allí, pero el volcado será extremadamente lento, más teniendo en cuenta la velocidad media de captura obtenida en las pruebas.

5.7.3.2. Tamaño total de la herramienta

Al tratarse de un ejecutable, el tamaño de Magnet RAM Capture es pequeño, un total de 108 KB de espacio en disco. Además, este es el tamaño total de la herramienta, pues no necesita otros archivos ni instalación para funcionar.

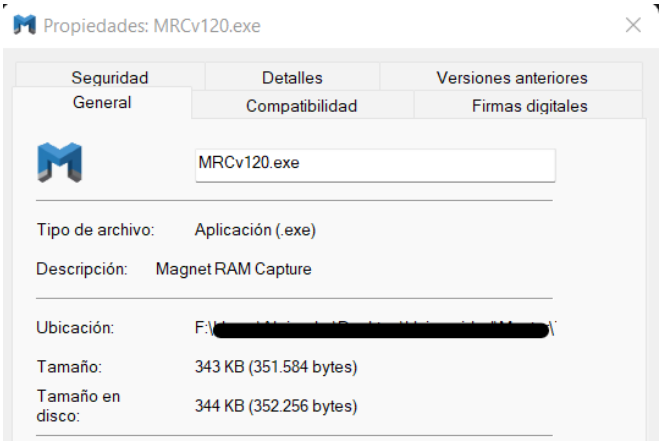


Figura 94. Tamaño total de la herramienta Magnet RAM Capture

5.7.3.3. Tipo de licencia

Como ya se ha detallado anteriormente, Magnet RAM Capture es una herramienta comercial con licencia de uso gratuita. Para descargar la herramienta, se accede a la página principal de Magnet Forensics, se selecciona la opción *Resources -> Free Tools* del menú superior y se elige Magnet RAM Capture. A continuación, para descargar la herramienta, se rellena un formulario, más simple y con menos datos personales que otras herramientas, y se enviará un correo electrónico con el enlace de descarga a la cuenta indicada en el campo de correo.

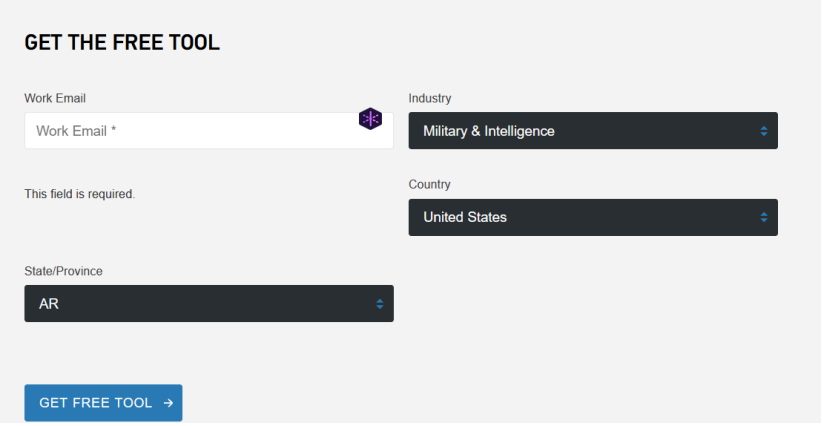


Figura 95. Cuestionario para descargar la herramienta Magnet RAM Capture

5.7.3.4. Funcionalidades adicionales

Magnet RAM Capture no dispone de ninguna funcionalidad adicional a la captura de memoria RAM y la segmentación del archivo.

5.7.3.5. Experiencia de usuario

Magnet RAM Capture no dispone de guía de usuario alguna sobre cómo utilizar la herramienta, pero tampoco es necesaria, simplemente se elige una ruta y un nombre de archivo y se pulsa en Start para que comience la captura. Al tratarse de una herramienta con interfaz gráfica, es más accesible que una con línea de comandos.

5.7.4. Conclusiones

En conclusión, Magnet RAM Capture es una herramienta sencilla con interfaz gráfica para obtener un volcado de datos de la memoria RAM, que permite dividir la captura en archivos del mismo tamaño de manera nativa. Sin embargo, estas son las únicas ventajas que posee, pues no dispone de ninguna opción adicional a la captura, lo cual no supondría ningún problema si no fuera porque el tiempo de captura en HDD es el más lento de todo el análisis con diferencia, 7 minutos, posiblemente por la incompatibilidad con el modo de 32 bits, el único que tiene la herramienta. Esto provoca que el equipo de pruebas no esté aprovechado, por lo que en una herramienta que no aporta otro valor más que la captura de memoria es un punto muy negativo que sea tan lenta.

Ventajas: Sencillez, facilidad de uso, portabilidad.

Desventajas: Velocidad de captura.

Valoración final: 5/10

5.8. Comparativa de herramientas de Windows

Una vez analizadas por separado todas las herramientas de Windows, se muestra a continuación una tabla en la que se indican las características cualitativas y cuantitativas de cada herramienta y su valoración final, según el análisis previo de cada una. Se ha decidido centrar el apartado del impacto en el rendimiento en la velocidad del disco duro, pues es el factor que más varía entre herramientas.

Herramienta	Vel. captura HDD	Vel. captura SSD	Impacto disco HDD	Impacto disco SSD	Opciones adicionales de captura	Portabilidad	Tamaño total	Licencia	Funcionalidades adicionales	Experiencia de usuario	Valoración final
FTK Imager	2m 29s	36s	110MB/s	417MB/s	Archivo de paginación, fichero AD1	Requiere instalación	112MB	Comercial, descarga gratuita	Visualización de evidencias digitales, duplicado de discos físicos	Interfaz gráfica, guía de usuario en PDF	**8**
OSForensics	3m 38s	47s	77MB/s	417MB/s	Ninguna	Requiere instalación	396MB	Comercial, prueba gratuita 30 días	Suite forense completa	Interfaz gráfica, guía de ayuda	**6,5**
WinPMem	2m 43s	20s	101MB/s	570MB/s	3 modos de captura: PTE, MmMapIoSpace, ruta memoria física	Ejecutable	515KB	Open Source	Ninguna	Línea de comandos, opciones complejas	**9**
Belkasoft	3m 5s	24s	90MB/s	726MB/s	Ninguna	Ejecutable	1,52MB	Comercial, descarga gratuita	Ninguna	Interfaz gráfica, intuitiva	**7**
Winen	2m 58s	1m 16s	77MB/s	230MB/s	Niveles de compresión, segmentar la captura	Ejecutable	408KB	Comercial, sin versión gratuita	Calcular el hash, opciones de granularidad, información forense	Línea de comandos, captura guiada	**7,2**
Win64dd	3m 44s	16s	72,5MB/s	773MB/s	Ficheros de volcado de errores, 3 modos de captura	Ejecutable	108KB	Comercial, gratuita	Calcular el hash, enviar la captura a un servidor en red local	Línea de comandos, ejemplos de uso	**8,5**
Magnet	7m 7s	49s	47MB/s	284MB/s	Segmentar la captura	Ejecutable	343KB	Comercial, descarga gratuita	Ninguna	Interfaz gráfica, intuitiva	**5**

Tabla 2. Comparativa de herramientas de Windows

Una vez comparadas en la tabla, en general, la velocidad de captura tanto en HDD como en SSD es constante, salvo en algunas excepciones. En el caso de HDD, Magnet RAM Capture es la más lenta con mucha diferencia, muy posiblemente por la utilización del modo de 32 bits de la herramienta, el único disponible. En cuanto a SSD, destaca la escasa compatibilidad que parece presentar Winen, superando el minuto de captura. También destaca win64dd, por lo contrario, su gran velocidad de captura en SSD.

En cuanto al impacto en el rendimiento, todas tienen un impacto similar, obviamente aprovechando mejor las altas velocidades de un disco SSD. El impacto en CPU y memoria es similar, por eso no se ha incluido en la tabla. Como este valor está relacionado con la velocidad de captura, sorprende la velocidad del disco duro en el caso de Magnet RAM Capture, así como la alta velocidad de FTK Imager, que aprovecha al máximo un disco HDD. En el terreno del SSD, sorprende que Magnet RAM Capture tenga un impacto en el disco tan bajo, pero que no sea una captura excesivamente lenta, a comparación con los datos de la prueba en HDD.

Respecto a opciones de captura adicional, hay alguna que no tiene ninguna, y que simplemente vuelcan toda la memoria en un archivo. Curiosamente, las herramientas de línea de comandos tienen más opciones de captura que las de interfaz gráfica, más incluso que las suites forenses. Las opciones más repetidas son la posibilidad de segmentar la captura en ficheros de mismo tamaño y poder elegir tres modos de captura distintos.

Sobre el método de ejecución se observa que, salvo el caso de FTK Imager y OSForensics, el resto son herramientas ejecutables que no admiten instalación. Estas dos herramientas son suites forenses cuyo principal objetivo no es capturar memoria, por lo que es esperable que se deban instalar para funcionar correctamente.

Los tamaños de las herramientas son también similares, notándose una clara diferencia entre las herramientas instalables y los ejecutables. En este último grupo destaca el caso de Belkasoft RAM Capturer, que ocupa bastante más que el resto, sobre todo si se compara con una herramienta de interfaz gráfica similar como Magnet RAM Capture, que ocupa más de 1MB menos de espacio.

En cuanto al tipo de licencia, destaca WinPMem como única representante de herramienta open source, pues el resto son herramientas con licencia comercial. Salvo el caso de Winen, que no tiene versión gratuita; y de OSForensics, que ofrece 30 días de prueba, las demás son de descarga y uso gratuito, pero con licencia comercial y software cerrado.

Respecto a las funcionalidades adicionales que no se relacionan con la adquisición de memoria, destacan las suites forenses, lo cual es esperable, teniendo en cuenta que el volcado de memoria es una característica secundaria de estas herramientas. Un total de 3 herramientas no disponen de ninguna opción adicional, mientras que la opción más repetida entre las demás es la de calcular el hash de la evidencia obtenida, funcionalidad muy ligada al análisis forense.

Por último, sobre la experiencia de usuario, destacar que ninguna de las herramientas es especialmente difícil de utilizar, si bien es cierto que los modos de captura de WinPMem y win64dd son complejos y no tienen documentación, la utilización es sencilla. Casi todas proporcionan algún tipo de ayuda al usuario, como las suites forenses, que son las mejor explicadas, con extensas guías de usuario en formato PDF o de ventana de ayuda. Las

herramientas de línea de comandos también aportan algún tipo de facilidad al usuario, como el caso de Winen y su captura guiada, indicando qué valor introducir para poder realizar la adquisición; o el caso de win64dd, que cuenta con ejemplos de ejecución de la herramienta.

A la vista de estos resultados y la valoración final, puede afirmarse que la mejor herramienta de adquisición de datos de la memoria RAM en Windows es WinPMem, pero no por mucha diferencia. Esta herramienta consigue ser la segunda más rápida en captura tanto en HDD como en SSD, lo cual no está nada mal, sin embargo dispone de otras características que la hacen destacar respecto al resto. Primero, es la única herramienta completamente open source de todas las analizadas, las demás son comerciales, ya sean gratuitas o de pago. Entre sus opciones adicionales se encuentra la posibilidad de elegir el modo de captura, una opción muy interesante para personalizar el volcado de datos. Además, es muy intuitiva y fácil de utilizar, con una ayuda descriptiva y bien explicados todos los parámetros que se pueden utilizar.

En segunda posición y muy cerca de WinPMem se encuentra win64dd, herramienta similar, que también cuenta con los tres modos de captura, pero además cuenta con muchas más opciones adicionales de captura. Permite enviar la captura por red, calcular el hash de la evidencia o volcar informes de errores de Microsoft. Los motivos por los cuales no es la mejor opción es porque primero, actualmente es bastante difícil de encontrar, porque no se puede obtener desde la página oficial de Moonsols; y porque se trata de una herramienta comercial, no es open source de código libre.

Por último, en tercera posición quedaría FTK Imager. Esta es seguramente la herramienta más conocida de todas las analizadas, siendo además de las más utilizadas para obtener memoria y visualizar información de evidencias digitales. No obstante, esto es un análisis de herramientas para adquirir memoria RAM, por lo que si existen herramientas con más opciones y funcionalidades para ello, estarán en mejor posición y serán más recomendables para esta tarea.

6. Herramientas de Linux

El segundo grupo de herramientas que se analizará será el formado por las utilidades que son compatibles con el sistema operativo Ubuntu en su versión 20.10. Se trata de un total de tres herramientas, siendo todas ejecutadas mediante línea de comandos. La forma general que utilizan las herramientas para capturar la memoria en Linux es instalando un módulo de kernel cargable (LKM), que proporciona la funcionalidad de acceso a la ruta del sistema /dev/mem, que contiene la información de la memoria física. Sin embargo, debe utilizarse con cuidado y eliminar el módulo tras su utilización, pues esta ruta está generalmente protegida para ofrecer seguridad ante modificaciones directas de la memoria, que pueden conllevar problemas graves de inestabilidad.

Es importante tener en cuenta que las pruebas solo han podido realizarse en SSD, que es donde está instalada la máquina virtual de Ubuntu 20.10, por lo que los valores serán comparados con Windows en SSD. También se debe tener en cuenta que el tamaño de la memoria es menos de la mitad de Windows: 6,6 GB frente a los 16 GB de Windows.

A continuación se analizarán cada una de las tres herramientas por separado, para después compararlas entre sí.

6.1. LiME

La primera herramienta de Linux que se va a analizar se trata de Linux Memory Extractor (LiME), en su versión 5.0 de marzo de 2021.

6.1.1. Descripción

LiME es una herramienta open source de línea de comando desarrollada inicialmente por Joe Sylve y mantenida en la actualidad por el equipo de 504ensicsLab. En sus comienzos en 2012 se conocía como DMD, pero pronto pasó a llamarse LiME. Esta herramienta es un módulo de Kernel cargable (LKM), que permite la adquisición de memoria volátil de dispositivos Linux y basados en Linux, como Android. Esto convierte a LiME en una herramienta única, pues es la primera que permite capturas de este tipo en dispositivos Android. Además, minimiza la interacción entre los procesos que trabajan en espacio de usuario y de kernel, lo que proporciona capturas más seguras desde el punto de vista forense que otras herramientas de adquisición de memoria [25].

```
insmod ./lime.ko "path=<outfile | tcp:<port>> format=<raw|padded|lime> [digest=<digest>] [dio=<0|1>]"

path (required):     outfile ~ name of file to write to on local system (SD Card)
                     tcp:port ~ network port to communicate over

format (required):   padded ~ pads all non-System RAM ranges with 0s
                     lime ~ each range prepended with fixed-size header containing address space info
                     raw ~ concatenates all System RAM ranges (warning : original position of dumped

digest (optional):   Hash the RAM and provide a .digest file with the sum.
                     Supports kernel version 2.6.11 and up. See below for
                     available digest options.

compress (optional): 1 ~ compress output with zlib
                     0 ~ do not compress (default)

dio (optional):      1 ~ attempt to enable Direct IO
                     0 ~ do not attempt Direct IO (default)

localhostonly (optional):  1 ~ restricts the tcp to only listen on localhost,
                           0 ~ binds on all interfaces (default)

timeout (optional): 1000 ~ max amount of milliseconds tolerated to read a page (default).
                           If a page exceeds the timeout all the memory region are skipped.
                      0 ~ disable the timeout so the slow region will be acquired.

                           This feature is only available on kernel versions >= 2.6.35.
```

Figura 96. Opciones principales de LiME

Para realizar una captura completa de la memoria con LiME, primero se debe compilar el programa con el makefile proporcionado, y una vez compilado se generará un módulo único para el kernel del dispositivo en el que se compiló. Después, se ejecuta el comando de Linux insmod, que instala un módulo del Kernel externo en el equipo, y se indican un nombre, un destino y un formato para la evidencia. Al terminar, se podrá acceder al archivo de memoria creado y comprobar que efectivamente, se vuelca todo el contenido de la memoria, 7 GB de tamaño total.

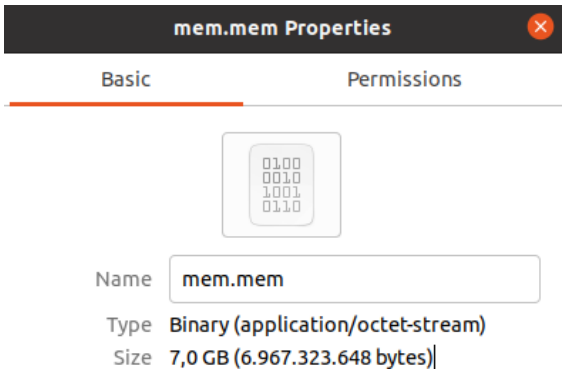


Figura 97. Tamaño captura de la memoria en LiME

6.1.2. Características principales

En este apartado se analizarán las características principales de LiME.

6.1.2.1. Velocidad de obtención del volcado de datos.

Para la obtención del tiempo de ejecución se ha utilizado el comando nativo de Linux *time*, que muestra el tiempo de ejecución de un comando, lo que devolverá un resultado más preciso que el uso de una herramienta externa.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **6,870 segundos**, sin margen de error, al tratarse de un tiempo dado por el sistema.

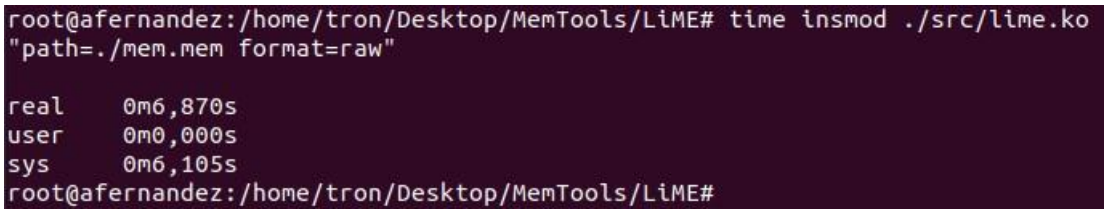


Figura 98. Primera captura con LiME

En la **segunda prueba**, el tiempo total ha sido de **6,641 segundos**, sin margen de error.

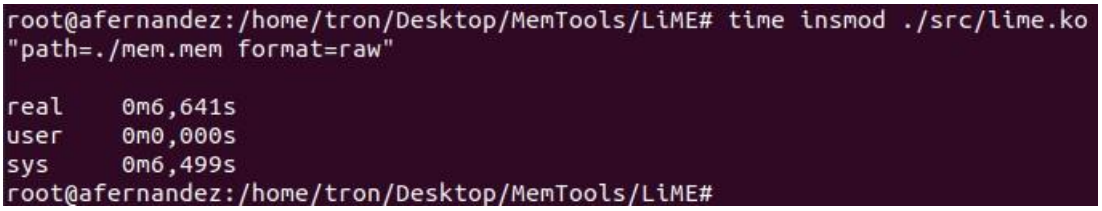


Figura 99. Segunda captura con LiME

En la **tercera prueba**, el tiempo ha sido de **6,343 segundos**, sin margen de error, lo que la convierte en la mejor prueba hasta ahora.

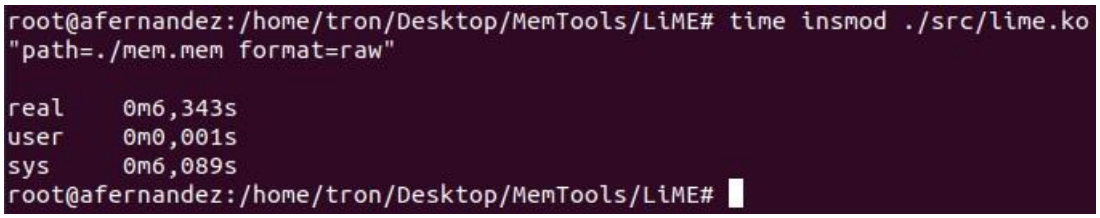


Figura 100. Tercera captura con LiME

La media de **duración de captura en SSD** para la herramienta **LiME** es de **6,618 segundos,** sin margen de error.

Como se puede observar, los resultados obtenidos con LiME son muy estables, siendo el valor determinante entre pruebas un factor de milésimas de segundo.

6.1.2.2. Impacto en el rendimiento del equipo

Para observar el rendimiento en el equipo, se ha utilizado la utilidad HTOP, que muestra información similar al administrador de tareas de Windows, pero con más opciones.

Durante la captura, el rendimiento del equipo se ha visto afectado por la herramienta en gran medida. El uso de CPU ha aumentado hasta llegar a un 70%, mientras que la memoria apenas se ha visto afectada, indicando un 0% de uso de memoria. Una desventaja es que no se muestra el uso del disco duro durante la prueba.

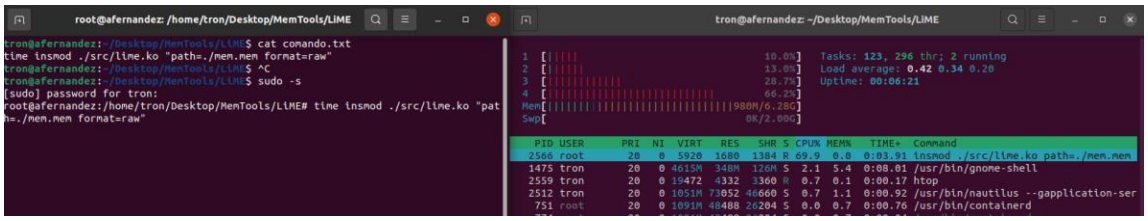


Figura 101. Impacto en el rendimiento SSD en LiME

6.1.2.3. Opciones adicionales de captura

LiME dispone de varias opciones adicionales de captura, empezando por la posibilidad de guardar la captura en el equipo local o tarjeta SD en caso de teléfono móvil, o enviarla a través de la red especificando el puerto TCP con el que comunicarse. Además, se permite modificar la salida de la captura con 3 formatos distintos. El modo relleno hace lo que su propio nombre indica,rellena los espacios que no corresponden a memoria RAM del sistema con 0; el modo lime añadea cada rango un encabezado fijo con la información del espacio de direcciones asignado; y el modo en bruto vuelca todo el rango de memoria del sistema.

```
path (required):     outfile ~ name of file to write to on local system (SD Card)
                     tcp:port ~ network port to communicate over

format (required):   padded ~ pads all non-System RAM ranges with 0s
                     lime ~ each range prepended with fixed-size header containing address space info
                     raw ~ concatenates all System RAM ranges (warning : original position of dumped
```

Figura 102. Opciones adicionales de captura en LiME

6.1.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta LiME.

6.1.3.1. Portabilidad

Se trata de una herramienta que consiste en una carpeta con los binarios del programa listos para ser compilados. Esto reduce su portabilidad, pues para poder funcionar en otro equipo distinto, se debe recompilar de nuevo toda la herramienta. No obstante, esto es algo esperable si se compara con Windows, pues el entorno Linux es mucho más abierto y con configuraciones del kernel distintas que en el caso del sistema operativo de Microsoft, en el que los componentes software se mantienen entre dispositivos.

6.1.3.2. Tamaño total de la herramienta

El tamaño total de LiME se divide en dos componentes principales: por un lado está el tamaño de todos los binarios sin compilar, y por otro está el módulo del kernel compilado. Con este módulo

basta para poder ejecutar el programa, pero antes se debe compilar en el equipo que se desee adquirir la memoria, pues el kernel de Linux es específico de cada distribución.

El tamaño de todos los binarios es de 153,5 KB de espacio en el disco.

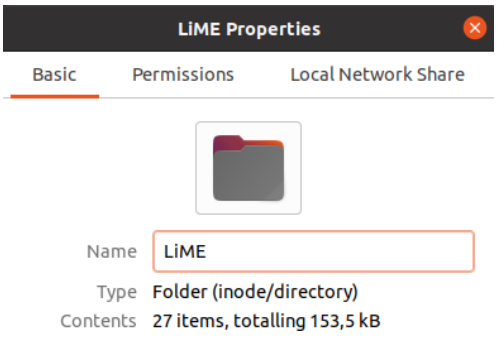


Figura 103. Tamaño binarios de LiME

El tamaño del módulo del kernel para Ubuntu 20.10 es de 21,5 KB.

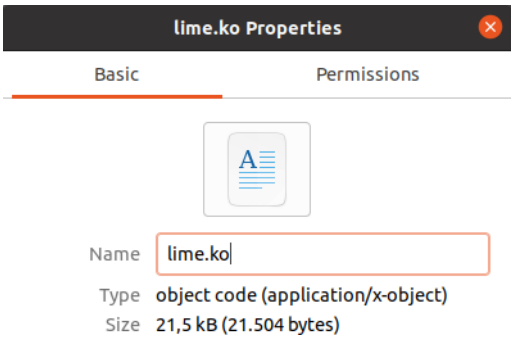


Figura 104. Tamaño módulo del kernel de LiME

6.1.3.3. Tipo de licencia

Como ya se ha mencionado, LiME es una herramienta open source. Actualmente, se encuentra disponible en el repositorio de Github de 504ensicsLab, con licencia GPL 2.0. Para utilizarla simplemente se clona el repositorio y se compilan los binarios descargados.

6.1.3.4. Funcionalidades adicionales

LiME dispone de algunas funcionalidades adicionales a la adquisición de memoria RAM. Una de las opciones permite calcular el hash de la evidencia obtenida, en los algoritmos más comunes como SHA-256 o MD5. Otra opción es poder comprimir la evidencia mediante el algoritmo zlib. Es interesante el método de habilitar el Direct IO. Este método permite saltarse el cacheado en memoria y escribir directamente en el disco duro, lo que ralentizará las operaciones, pero es muy útil en entornos con poca memoria volátil disponible, pues permite contar con más capacidad, a costa de la velocidad de acceso [26]. Por último, se puede modificar el tiempo que el módulo LiME esperará a leer una página de la memoria, por defecto activado en 1 segundo, si tarda más de ese tiempo, saltará a la siguiente.

```
digest (optional):   Hash the RAM and provide a .digest file with the sum.
                     Supports kernel version 2.6.11 and up. See below for
                     available digest options.

compress (optional): 1 ~ compress output with zlib
                     0 ~ do not compress (default)

dio (optional):      1 ~ attempt to enable Direct IO
                     0 ~ do not attempt Direct IO (default)

localhostonly (optional):  1 ~ restricts the tcp to only listen on localhost,
                           0 ~ binds on all interfaces (default)

timeout (optional): 1000 ~ max amount of milliseconds tolerated to read a page (default).
                           If a page exceeds the timeout all the memory region are skipped.
                      0 ~ disable the timeout so the slow region will be acquired.
```

Figura 105. Funcionalidades adicionales de LiME

6.1.3.5. Experiencia de usuario

La herramienta LiME dispone de una guía de usuario en la que se detalla bastante información sobre la herramienta, sus distintas opciones y prerrequisitos necesarios para su ejecución. Sin embargo, al tratarse de una herramienta que debe ser compilada previamente y ejecutada por línea de comandos, su facilidad de uso es menor. Además, aunque exista documentación, el uso de esta herramienta requiere conocimientos básicos de Linux y de compilación, porque la información que se muestra puede llegar a resultar un tanto confusa.

```
# LiME - Linux Memory Extractor
## Contents
* [Compiling](#Compile)
  * [Linux](#Linux)
  * [External](#External)
  * [Debug](#Debug)
  * [Symbols](#Symbols)
  * [Android](#Android)
* [Usage](#Usage)
  * [Parameters](#Params)
  * [Acquisition of Memory over TCP](#TCP)
  * [Acquisition of Memory to Disk (SD-Card)](#Disk)
* [LiME Memory Range Header Version 1 Specification](#Spec)

## Compiling LiME <a name="Compile"/>
### Linux <a name="Linux"/>
LiME is a Loadable Kernel Module (LKM).  LiME ships with a default Makefile that should be suitabl
e for compilation on most modern Linux systems.

For detailed instructions on using LKM see https://www.kernel.org/doc/Documentation/kbuild/modules
.txt.

### External <a name="External"/>
LiME can be compiled externally from the target in order to provide a more forensically sound and
secure method. Follow this [guide](./external_modules.md) to learn how.

### Debug  <a name="Debug"/>
When compiling LiME with the default Makefile, using the command “make debug” will compile a LiME
module with extra debug output.  The output can be read by using the dmesg command on Linux.

### Symbols  <a name="Symbols"/>
@@@
                                                                              1,1           Top
```

Figura 106. Guía de usuario de LiME

6.1.4. Conclusiones

En conclusión, LiME es una herramienta open source para obtener un volcado de datos de la memoria RAM en entornos Linux, incluidos smartphones. Es muy rápida capturando memoria, incluso dentro de una máquina virtual con menos recursos, y dispone de varias opciones adicionales a la captura que son interesantes desde el punto de vista forense, como calcular el

hash o enviar los datos a través de la red. Es un poco compleja de utilizar, y el método de cargar los módulos en el kernel puede resultar un concepto avanzado, pero detrás de esto se encuentra una de las herramientas más potentes y completas de captura de memoria RAM.

Ventajas: Velocidad de captura, opciones adicionales, compatibilidad con smartphones.

Desventajas: Dificultad de utilización, ayuda compleja.

Valoración final: 9/10

6.2. Memdump

La siguiente herramienta que se va a analizar se trata de Memdump, en su versión 1.01 de octubre de 2013.

6.2.1. Descripción

Memdump es una herramienta open source empaquetada en el core de Ubuntu y desarrollada por Wietse Venema, investigador de IBM. Esta herramienta vuelca el contenido de la ruta /dev/mem a la salida estándar en formato stream, saltándose los huecos en el mapa de memoria [27]. Por defecto, muestra el contenido en bruto, pero se puede especificar que obtenga además información sobre la disposición de la memoria como la página o el rango de direcciones. Se recomienda enviar la captura a través de la red, para que no se modifique la memoria local del equipo.

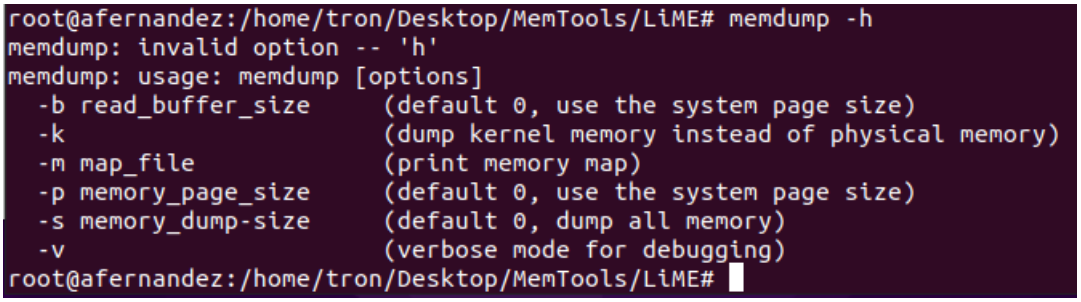


Figura 107. Pantalla principal de Memdump

Para realizar una captura completa de la memoria con Memdump, simplemente se lanza el comando y empezará a mostrar información por pantalla. Para volcarlo a un archivo, se redirige la salida estándar a un archivo en una ruta determinada.

6.2.2. Características principales

En este apartado se analizarán las características principales de Memdump.

6.2.2.1. Velocidad de obtención del volcado de datos.

Para poder analizar esta herramienta, se debe conocer previamente el funcionamiento de la misma. Memdump vuelca por defecto el contenido de la ruta */dev/mem*, donde se almacena la memoria física del sistema. En las últimas versiones de Ubuntu, por seguridad, esta ruta está protegida para permitir el acceso solamente al primer megabyte de datos, o en algunos casos ni siquiera es accesible al usuario, sin importar su nivel de privilegios. Por lo tanto, al iniciar la captura con Memdump, esta vuelca el primer megabyte de datos en un archivo, y luego continúa durante un tiempo indefinido, pero sin mostrar más información.

En resumen, no ha sido posible la adquisición de datos de la memoria RAM con Memdump, solamente se ha obtenido un fichero de 1 MB de tamaño, que es lo que permite el kernel del sistema.

6.2.2.2. Impacto en el rendimiento del equipo

Durante el tiempo que se ha mantenido en ejecución la herramienta hasta concluir que no podía acceder a la memoria, el impacto en el rendimiento se ha centrado en la CPU, siendo el uso de esta del 100% en el núcleo número 3, de 4 disponibles. Igual que pasaba con LiME, no es posible ver el impacto en el disco duro, y el impacto en la memoria es del 0%.

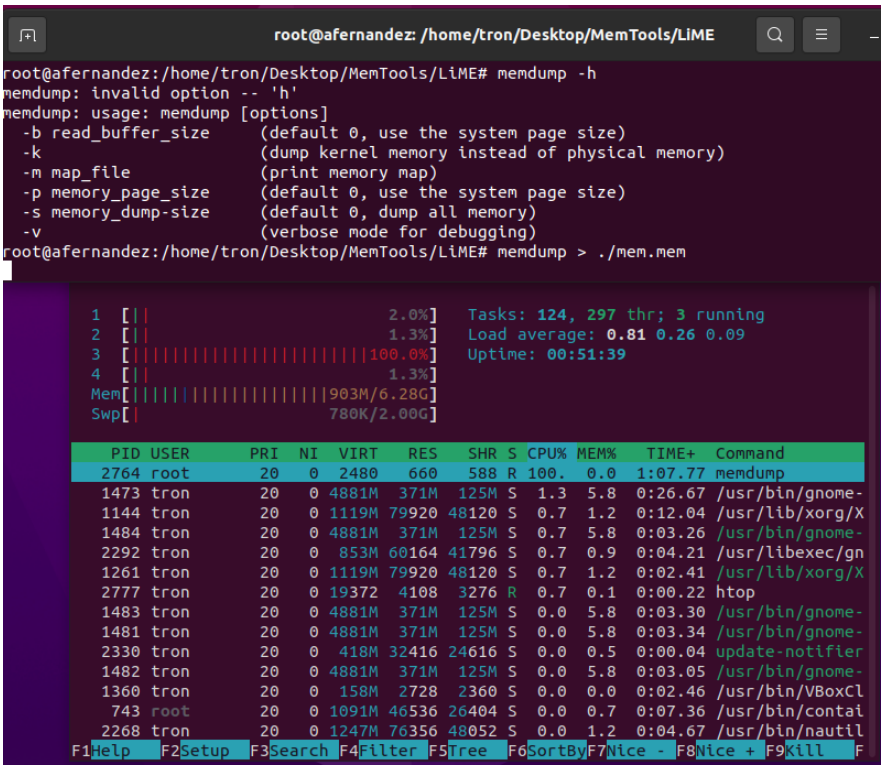


Figura 108. Impacto en el rendimiento SSD en Memdump

6.2.2.3. Opciones adicionales de captura

Memdump dispone de varias opciones adicionales de captura de datos de la memoria RAM. Es posible establecer el tamaño del búfer de lectura, pero por defecto utiliza el tamaño de página del sistema, para volcar una página cada vez. También se puede volcar la memoria del kernel, disponible en la ruta /dev/kmem, así como mostrar un mapa de la memoria física. Por último, Memdump permite modificar el tamaño de la página de la memoria y el tamaño del volcado que se obtendrá.

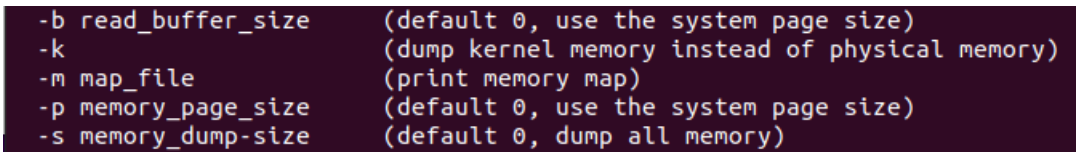


Figura 109. Opciones adicionales de captura de Memdump

6.2.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta Memdump.

6.2.3.1. Portabilidad

Memdump es una herramienta que está instalada por defecto en Ubuntu, pero se puede descargar el paquete desde la página oficial del manual de memdump en Ubuntu, para poder llevar la herramienta en una memoria extraíble USB. Sin embargo, aunque se descargue, es necesario compilar los binarios en el equipo que se va a utilizar, lo que reduce la portabilidad.

6.2.3.2. Tamaño total de la herramienta

Como Memdump viene instalada en el core de Ubuntu, el tamaño no es algo de lo quepreocuparse. No obstante, si se desea, se puede descargar el paquete con la herramienta desde la página oficial de Ubuntu. De esta forma, se obtiene el tamaño del paquete con los binarios de Memdump, los cuales ocupan un tamaño comprimido de 12,7 KB y de 39,1 KB extraídos.

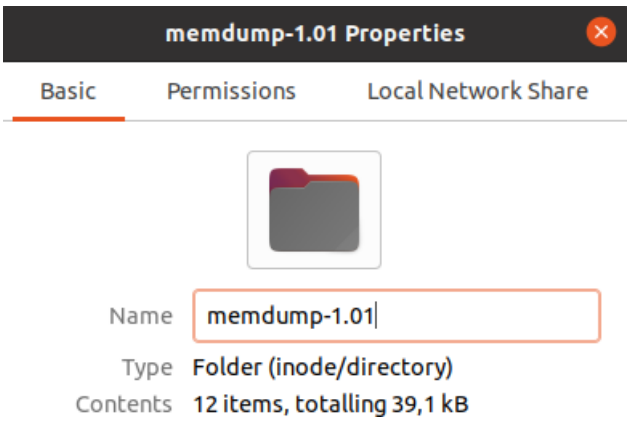


Figura 110. Tamaño total de la herramienta Memdump

6.2.3.3. Tipo de licencia

Como ya se ha detallado anteriormente, Memdump es una herramienta open source con licencia IBM Public License. La herramienta está instalada por defecto en el core de Ubuntu, pero si se desea instalar en otro sistema operativo o disponer de los binarios por cualquier razón, en la página oficial del manual de Ubuntu, se puede descargar el paquete de forma directa, ya que se trata de una herramienta open source.

6.2.3.4. Funcionalidades adicionales

Memdump no dispone de funcionalidades adicionales a la captura de memoria RAM, puesto que se trata de un módulo exclusivo para ello.

6.2.3.5. Experiencia de usuario

Memdump dispone de guía de usuario en forma de páginas del manual de Linux, con el comando *man memdump* se puede consultar la guía de ayuda de la herramienta. Además, se puede consultar la versión reducida de la ayuda si se introduce el comando *memdump* con el parámetro *-h*. Esto muestra los principales parámetros que se pueden utilizar en la herramienta, pero sin explicarlos en detalle como sí hace *man*. La adquisición de datos de la memoria es muy sencilla, pues simplemente se debe lanzar la herramienta y comenzará a volcar datos por pantalla. Para especificar un destino, se pueden utilizar redirecciones de salida de terminal.

6.2.4. Conclusiones

En conclusión, Memdump es una herramienta simple para capturar memoria RAM en entornos Linux. Sin embargo, no ha sido posible completar ninguna captura por la limitación del kernel al acceso a la ruta /dev/mem que contiene la información de la memoria física en uso. No obstante, esta herramienta funcionará en versiones de Linux más antiguas que no disponga de esta limitación. Entre sus características secundarias destaca su escaso tamaño, sus múltiples opciones de personalización de tamaño de páginas de memoria para la captura y su ayuda al usuario.

Ventajas: Opciones de captura, experiencia de usuario.

Desventajas: No funciona en equipos modernos.

Valoración final: 2/10

6.3. Fmem

La última herramienta que se va a analizar se trata de Fmem, en su versión 1.6.0 de julio de 2019.

6.3.1. Descripción

Fmem es una herramienta de adquisición de memoria volátil open source con licencia GPL 2.0. Actualmente, está mantenida en un repositorio en Github por Nate Brune, después de que cerrara el proyecto original . Funciona instalando un módulo de kernel cargable, creando una copia de la ruta bloqueada por el sistema /dev/mem, en la ruta /dev/fmem. Esta nueva ruta es una copia exacta de la original, pero sin las restricciones de acceso (1MB de volcado), por lo que una vez creada se puede acceder a ella y leer o cambiar el contenido de manera segura, pues no se modifica directamente la memoria física, solo una copia de la misma. Como funcionalidad interesante, esta herramienta permite la captura infinita de la memoria si no se establece un límite de datos a leer.

```
tron@afernandez:~/Desktop/MemTools/fmem$ make
rm -f *.o *.ko *.mod.c Module.symvers Module.markers modules.order \.*.o.cmd \.*.ko.cmd \.*.o.d
rm -rf \.tmp_versions
make -C /lib/modules/`uname -r`/build KBUILD_EXTMOD=`pwd` modules
make[1]: Entering directory '/usr/src/linux-headers-5.8.0-59-generic'
  CC [M]  /home/tron/Desktop/MemTools/fmem/lkm.o
  LD [M]  /home/tron/Desktop/MemTools/fmem/fmem.o
  MODPOST /home/tron/Desktop/MemTools/fmem/Module.symvers
  CC [M]  /home/tron/Desktop/MemTools/fmem/fmem.mod.o
  LD [M]  /home/tron/Desktop/MemTools/fmem/fmem.ko
make[1]: Leaving directory '/usr/src/linux-headers-5.8.0-59-generic'
tron@afernandez:~/Desktop/MemTools/fmem$ sudo ./run.sh
rmmod: ERROR: Module fmem is not currently loaded
Module: insmod fmem.ko a1=0xffffffffbc8a6c10 : OK
Device: /dev/fmem
----Memory areas: -----
tron@afernandez:~/Desktop/MemTools/fmem$ sudo time dd if=/dev/fmem of=mem.mem bs=1MB count=6644
dd: error writing 'mem.mem': No space left on device
5514+0 records in
5513+0 records out
5513433088 bytes (5,5 GB, 5,1 GiB) copied, 27,0794 s, 204 MB/s
Command exited with non-zero status 1
0.00user 25.40system 0:27.07elapsed 93%CPU (0avgtext+0avgdata 3404maxresident)k
120inputs+10768432outputs (0major+333minor)pagefaults 0swaps
tron@afernandez:~/Desktop/MemTools/fmem$ sudo time dd if=/dev/fmem of=mem.mem bs=1MB count=6644
6644+0 records in
6644+0 records out
6644000000 bytes (6,6 GB, 6,2 GiB) copied, 24,0107 s, 277 MB/s
0.00user 23.97system 0:24.01elapsed 99%CPU (0avgtext+0avgdata 3344maxresident)k
8inputs+12976576outputs (1major+332minor)pagefaults 0swaps
tron@afernandez:~/Desktop/MemTools/fmem$
```

Figura 111. Procedimiento de captura con Fmem

Para realizar una captura completa de la memoria con Fmem, primero se debe compilar el programa con el makefile proporcionado, y una vez compilado se generará un módulo único para el kernel del dispositivo en el que se compiló. Después, se ejecuta el script run.sh, que lanzará el comando *insmod* para instalar un módulo del Kernel externo en el equipo. Por último, se utiliza el comando de Linux *dd*, para copiar los datos de la ruta */dev/fmem* al destino que se desee, indicando un nombre, el tamaño del bloque y el tamaño de la memoria a capturar en MB. Al terminar, se podrá acceder al archivo de memoria creado y comprobar que se vuelca todo el contenido de la memoria especificado, 6,6 GB de tamaño total.

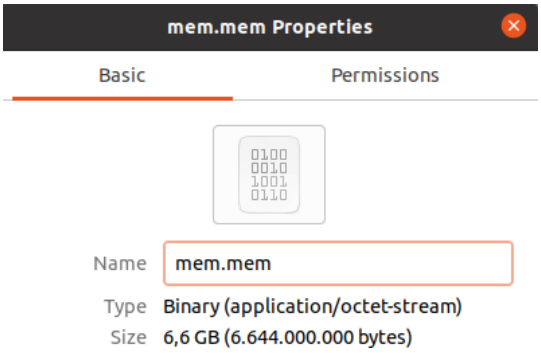


Figura 112. Tamaño captura de la memoria en Fmem

6.3.2. Características principales

En este apartado se analizarán las características principales de Fmem.

6.3.2.1. Velocidad de obtención del volcado de datos.

Para la obtención del tiempo de ejecución se ha utilizado el comando nativo de Linux *time*, que muestra el tiempo de ejecución de un comando, lo que devolverá un resultado más preciso que el uso de una herramienta externa.

En la **primera prueba** real con la herramienta, la adquisición de datos de la memoria completa ha durado un total de **24,01 segundos**, sin margen de error, al tratarse de un tiempo dado por el sistema.

```
tron@afernandez:~/Desktop/MemTools/fmem$ sudo time dd if=/dev/fmem of=mem.mem bs=1MB count=6644
6644+0 records in
6644+0 records out
6644000000 bytes (6,6 GB, 6,2 GiB) copied, 24,0107 s, 277 MB/s
0.00user 23.97system 0:24.01elapsed 99%CPU (0avgtext+0avgdata 3344maxresident)k
8inputs+12976576outputs (1major+332minor)pagefaults 0swaps
```

Figura 113. Primera captura con Fmem

En la **segunda prueba**, el tiempo total ha sido de **24,47 segundos**, sin margen de error.

```
tron@afernandez:~/Desktop/MemTools/fmem$ sudo time dd if=/dev/fmem of=mem.mem bs=1MB count=6644
6644+0 records in
6644+0 records out
6644000000 bytes (6,6 GB, 6,2 GiB) copied, 24,4732 s, 271 MB/s
0.02user 24.38system 0:24.79elapsed 98%CPU (0avgtext+0avgdata 3312maxresident)k
8inputs+12976584outputs (1major+334minor)pagefaults 0swaps
```

Figura 114. Segunda captura con Fmem

En la **tercera prueba**, el tiempo ha sido de **23,82 segundos**, sin margen de error, lo que la convierte en la mejor prueba hasta ahora.

```
tron@afernandez:~/Desktop/MemTools/fmem$ sudo time dd if=/dev/fmem of=mem.mem bs=1MB count=6644
6644+0 records in
6644+0 records out
6644000000 bytes (6,6 GB, 6,2 GiB) copied, 23,8209 s, 279 MB/s
0.00user 23.94system 0:24.12elapsed 99%CPU (0avgtext+0avgdata 3392maxresident)k
8inputs+12976576outputs (1major+335minor)pagefaults 0swaps
```

Figura 115. Tercera captura con Fmem

La media de **duración de captura en SSD** para Fmem es de **24,10 segundos,** sin margen de error.

6.3.2.2. Impacto en el rendimiento del equipo

En la propia captura, al terminar, se muestra una media de utilización de la CPU, que da una media del 99% de utilización. Si se emplea la herramienta HTOP, la misma que en el caso de LiME, se puede observar que la CPU aumenta hasta un 108% de utilización, mientras que la memoria marca un 0% de uso. El impacto en el disco no es mostrado por esta herramienta.

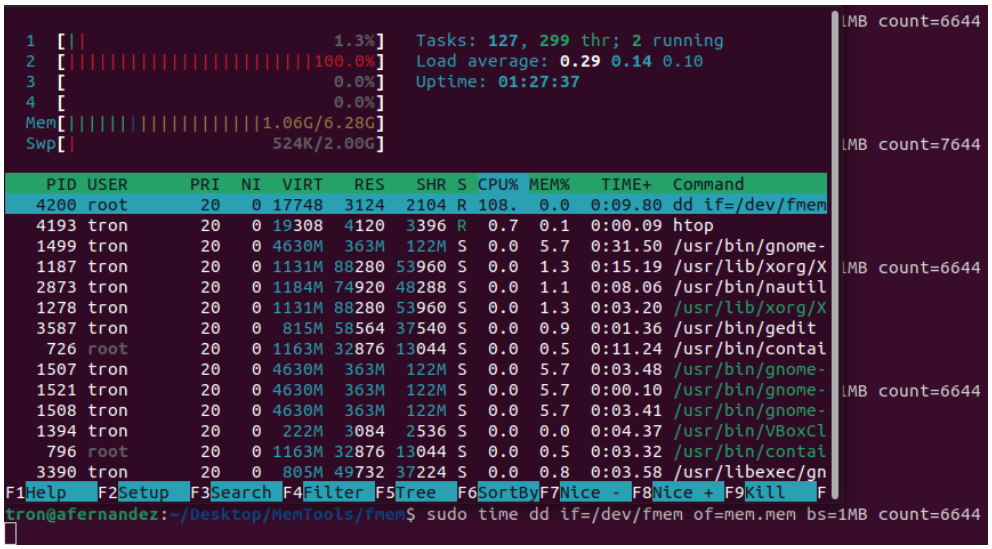


Figura 116. Impacto en el rendimiento SSD en Fmem

6.3.2.3. Opciones adicionales de captura

Fmem dispone de dos opciones adicional de captura, establecer el tamaño del bloque, que será la cantidad máxima de datos que se leerán de la memoria a la vez; y el tamaño de lectura de la memoria, que marcará el límite de datos a leer en total de la ruta /dev/fmem. Si no se indica este último parámetro, la herramienta capturará datos indefinidamente.

```
-----
Usage:

$ make

# ./run.sh

# dd if=/dev/fmem of=... bs=1MB count=...
```

Figura 117. Opciones adicionales de captura en Fmem

6.3.3. Características secundarias

En este apartado se analizarán las características secundarias que presenta Fmem.

6.3.3.1. Portabilidad

Similar a LiME, el núcleo de Fmem es el módulo de kernel cargable, por lo que este debe ser compilado en el equipo en el que se va a capturar la memoria, o de lo contrario no funcionará la herramienta. Esto reduce bastante su portabilidad, no obstante, es algo esperable si se compara con Windows, pues el entorno Linux es mucho más abierto y con configuraciones del kernel distintas que en el caso del sistema operativo de Microsoft, en el que los componentes software se mantienen entre dispositivos.

6.3.3.2. Tamaño total de la herramienta

El tamaño total de Fmem se divide en dos componentes principales: por un lado está el tamaño de todos los binarios sin compilar, y por otro está el módulo del kernel compilado. Con este módulo basta para poder ejecutar el programa, pero antes se debe compilar en el equipo que se desee adquirir la memoria, pues el kernel de Linux es específico de cada distribución.

El tamaño de todos los binarios es de 73,7 KB de espacio en el disco.

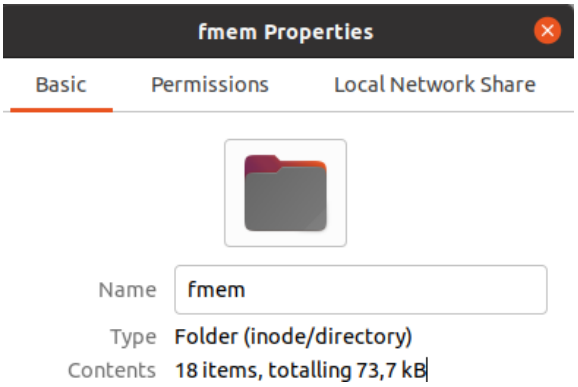


Figura 118. Tamaño de los binarios de Fmem

El tamaño del módulo del kernel de Fmem es de 13,8KB

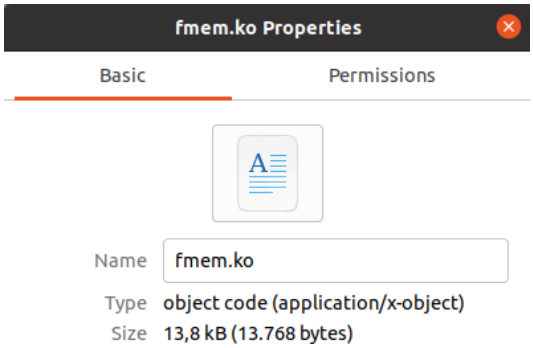


Figura 119. Tamaño del módulo del kernel de Fmem

6.3.3.3. Tipo de licencia

Como ya se ha mencionado, Fmem es una herramienta open source. Actualmente, se encuentra disponible en el repositorio de Github de NateBrune, con licencia GPL 2.0. Para utilizarla simplemente se clona el repositorio y se compilan los binarios descargados.

6.3.3.4. Funcionalidades adicionales

Fmem no dispone de funcionalidades adicionales a la captura de memoria, pues se centra en proporcionar un módulo de kernel para el sistema.

6.3.3.5. Experiencia de usuario

Fmem no dispone de guía de usuario alguna sobre cómo utilizar la herramienta, simplemente cuenta con un brevísimo Readme escrito por Nate Brune sobre cómo utilizar la herramienta, pero no se indica nada más. Sin embargo, la instalación, aunque no se aporte información, es muy sencilla, y la carga del módulo del kernel se hace de forma transparente al usuario.

```
fmem 1.6.0

This repo is was originally a github mirror of the original fmem module.
Later this repo became a maintained version of fmem to account for a changing Linux kernel.
Bug reports and patches welcome.

This module creates /dev/fmem device,
that can be used for dumping physical memory,
without limits of /dev/mem (1MB/1GB, depending on distribution)

Tested on i386 and x64, feel free to test it on
different architectures. (and send report please)

Cloned from linux/drivers/char/mem.c
(so GPL license apply)

Original name of this tool was fdump,
which was conflict with already existing tool,
so name was changed to fmem

2009,2010 niekt0@hysteria.sk

-----
Usage:

$ make

# ./run.sh

# dd if=/dev/fmem of=... bs=1MB count=...

-----
BUGS: if you do something like # dd if=/dev/fmem of=dump
      dd will never stop, even if there is no more physical RAM
      on the system. This is more a feature, because Linux kernel
      don't have stable API, and detection of mapped areas can be
      tricky on older kernels. Because primary usage for fmem is
      memory forensic, I think it is safer to specify
      amount of RAM by hand.
-----
```

Figura 120. Readme completo de Fmem

6.3.4. Conclusiones

En conclusión, Fmem es una herramienta aparentemente sencilla para adquirir la memoria física de un sistema Linux, pero que en realidad es bastante compleja de utilizar, en gran medida por la escasa información disponible sobre la herramienta. La captura no es muy rápida para el tamaño que hay que obtener, y no aporta ninguna opción adicional relevante a la captura de memoria. Sin embargo, la limitación de Linux sobre la ruta /dev/mem la convierten en una de las pocas herramientas que existen que crean un módulo de kernel cargable.

Ventajas: Open source, fácil instalación del LKM.

Desventajas: Lenta, pocas opciones de captura.

Valoración final: 5/10

6.4. Comparativa de herramientas de Linux

Una vez analizadas por separado todas las herramientas de Linux, se muestra a continuación una tabla en la que se indican las características cualitativas y cuantitativas de cada herramienta y su valoración final, según el análisis previo de cada una. Se ha decidido centrar el apartado del impacto en el rendimiento en la utilización de CPU, aunque no sea muy relevante, pues el apartado de la memoria es el mismo en los tres casos y el disco duro no se ha podido obtener.

Herramienta	Vel. Captura (SSD)	Impacto rendimiento	Opciones adicionales de captura	Portabilidad	Tamaño total	Licencia	Funcionalidades adicionales	Experiencia de usuario	Valoración final
LiME	6,618s	99%	Envío en red local, 3 modos de relleno	Necesita compilación local	153,5 KB (Binarios) 21,5 KB (LKM)	Open Source (GPL 2.0)	Hash, compresión, módulo Direct IO	Conceptos complejos, guía de usuario	**9**
Memdump	No aplica	100%	Tamaño del búfer y de página, volcar la memoria virtual	Módulo preinstalado	39,1 KB	Open Source (IBM Public License)	Ninguna	Manual de Linux, comando sencillo	**2**
Fmem	24,10s	108%	Tamaño del bloque, tamaño de la captura	Necesita compilación local	73,7 KB (Binarios) 13,8 (LKM)	Open Source (GPL 2.0)	Ninguna	Escasa información, instalación sencilla	**5**

Tabla 3. Comparativa de herramientas de Linux

A la vista de estos resultados, es bastante obvio que la mejor herramienta de adquisición de memoria RAM en entornos Linux es LiME. No solo es la más rápida entre las tres, también es la que más funcionalidades posee, como los modos de relleno de la memoria, la posibilidad de enviar el resultado por red local o la compresión de la evidencia resultante. Además, es una herramienta que actualmente está bajo soporte continuo de la comunidad, actualizando el repositorio de manera frecuente. Por último, permite la captura de memoria también en smartphones, lo que aumenta mucho su funcionalidad y utilidad.

Por otro lado, Memdump no es una herramienta recomendable para capturar memoria actualmente, ya que la mayoría de sistemas operativos Linux tienen bloqueado el acceso a /dev/mem.

En cuanto a Fmem, no es una mala opción ni mucho menos, pero existen alternativas mejores, y no aporta ninguna funcionalidad que la haga destacar frente al resto.

7. Comparativa general

Tras haber realizado la comparativa entre todas las herramientas, ahora se pueden comparar de manera general, evaluando sus puntos positivos y negativos, y eligiendo las mejores herramientas según sus funcionalidades y características. Para ello, se han seleccionado varias categorías, de forma que en cada una habrá una o varias herramientas, que serán las que mejor representen a ese grupo. Las categorías propuestas son las siguientes:

- Mejor herramienta para captura rápida
- Mejor herramienta para análisis forense
- Mejores opciones de captura
- Mejor portabilidad
- Mejor experiencia de usuario
- Mejor herramienta en general

A continuación se detallan todas las categorías con las herramientas más recomendables para cada una.

7.1. Mejor herramienta para captura rápida

En esta categoría se evalúa cuál es la mejor herramienta para realizar una captura rápida. La mejor candidata debería ser la más rápida tanto en un disco duro HDD como en un disco de estado sólido. Para este grupo se debe tener en cuenta que la captura en Linux es de tamaño reducido, 6,6GB frente a los 16GB capturados en Windows.

Por lo tanto, la herramienta de adquisición de memoria más rápida para un disco HDD es **FTK Imager**, mientras que para un disco SSD, es **win64dd.** Sin embargo, cada una de estas opciones es bastante peor en la captura con el otro tipo de disco, SSD en FTK Imager y HDD en win64dd. Si se busca una herramienta rápida pero que esté balanceada en captura en los dos tipos de disco, la opción más rápida de todas es **WinPMem,** que se coloca entre las dos herramientas mencionadas, siendo un poco peor que cada una en su mejor captura, pero que no llega a ser tan lenta en la peor captura de FTK Imager y win64dd.

Mención especial para **LiME** en capturas en SSD (no se ha probado en HDD, por lo que no se puede afirmar que sea más rápida que WinPMem u otras opciones) que, si se calcula el tiempo que tardaría en capturar 16GB, tardaría un tiempo aproximado de 16 segundos, lo que la colocaría como herramienta más rápida en entornos Linux.

7.2. Mejor herramienta para análisis forense

En esta categoría se evalúan las herramientas según sus características que puedan resultar útiles en una investigación forense. Funcionalidades como poder calcular el hash de la evidencia, analizar la captura obtenida o introducir información sobre el investigador encargado de la adquisición formarían parte de las características que se buscan en una herramienta enfocada al análisis forense.

Por lo tanto, la mejor herramienta para análisis forense sería, sin lugar a duda, **OSForensics.** Es bastante obvio el por qué esta herramienta es la mejor opción, puesto que es una suite forense completa y su principal objetivo es servir de base y reunir en una misma aplicación el máximo de aplicaciones forenses posibles. Otra opción en esta categoría sería la herramienta **Winen,** que

también dispone de varias opciones enfocadas al análisis forense, como calcular el hash del volcado de datos o insertar información forense en la captura. En este caso, salta a la vista que Winen forma parte de la instalación de EnCase, una de las mejores herramientas de análisis forense profesional.

7.3. Mejores opciones adicionales

En esta categoría se evalúa qué herramienta tiene las mejores opciones adicionales a la captura de datos de la memoria RAM y funcionalidades adicionales, no necesariamente relacionadas con el análisis forense. Entre las opciones adicionales de captura que se pueden encontrar están la posibilidad de segmentar el archivo final en partes más pequeñas de igual tamaño o elegir modos de captura distintos. Respecto a las funcionalidades adicionales, se valorará positivamente la posibilidad de enviar la captura por la red o comprimir el archivo de volcado para que ocupe menos espacio en disco.

En este caso, la mejor herramienta es **LiME**, muy igualada con **win64dd**. LiME permite la compresión de la evidencia obtenida, puede calcular el hash, enviar el volcado a través de la red local a otro equipo o servidor, dispone de 3 modos distintos de relleno de la captura y puede utilizar el modo Direct IO para facilitar la captura en entornos con poca memoria RAM. Todas las opciones mencionadas se complementan con la posibilidad de utilizar esta herramienta para obtener la memoria RAM de un dispositivo Android, no solo se limita a equipos de sobremesa o servidores Linux. En cuanto a win64dd, esta herramienta presenta funcionalidades similares, como el envío de la captura en la red o el cálculo del hash, pero además puede generar informes de errores de Microsoft, así como utilizar 3 modos distintos de captura.

7.4. Mejor portabilidad

En esta categoría se tiene en cuenta la portabilidad de la herramienta, el tamaño total que ocupa en disco y la facilidad para instalarla en el equipo propio o en otro, así como ejecutarla desde una unidad de memoria externa, como un pendrive USB. Claramente, una herramienta que no requiera de instalación y simplemente se trate de un ejecutable será lo ideal, pero también se debe resaltar su espacio, pues si ocupa mucho, no será todo lo útil que cabría esperar.

La mejor herramienta en temas de portabilidad es **win64dd,** seguida por **Fmem.** Win64dd es la herramienta más ligera de todas las analizadas en Windows, con un tamaño total de 106 KB, además de que se trata de un ejecutable, que se puede lanzar desde una terminal, ya sea desde el propio equipo o desde una unidad USB. El caso de Fmem es especial, porque aunque ocupe muy poco, solamente 73 KB de espacio en disco para los binarios y 13 KB el módulo de kernel, es necesaria la compilación en el equipo en que se va a obtener el volcado de datos, lo que resta portabilidad, pues se necesita un compilador de C para ejecutarla.

7.5. Mejor experiencia de usuario

En esta categoría se analiza la herramienta que es más fácil de utilizar, ya sea porque tiene menús claros y explicativos, o porque no tiene parámetros complicados para realizar una captura simple. Se valora que la herramienta tenga una guía de ayuda al usuario, que proporcione ejemplos de cómo realizar una captura, y que en general sea fácil de utilizar.

En este caso, la mejor experiencia de usuario la proporcionan las herramientas **Belkasoft RAM Capturer** y **Magnet RAM Capture.** Estas dos son herramientas muy similares en cuanto a experiencia de usuario, pues ambas son herramientas que interactúan con el usuario a través de interfaz gráfica, lo que las hace muy accesibles a cualquier usuario. Además, ambas se componen de un solo ejecutable, que no necesita instalación. Todo ello se combina con la facilidad de obtención de los datos, simplemente elegir una ruta de volcado, que se realiza a través del explorador de Windows en ambos casos, y pulsar en el botón capturar.

7.6. Mejor herramienta en general

Por último, en esta categoría se evalúa cuál es la mejor herramienta de todas las presentadas hasta ahora. Esta herramienta debe ser si no la mejor, de las mejores en todos los apartados, aportando funcionalidades que no estén presentes en otras herramientas, capturando los datos rápidamente, siendo portable y fácil de utilizar. La valoración numérica de cada herramienta da una idea de cuál es la mejor desde un punto de vista general, y en este apartado se dan las razones de la elección de esta valoración.

En general, la mejor herramienta para adquirir memoria volátil de un equipo es **WinPMem** para entornos Windows, y **LiME** para entornos Linux. Sería injusto para ambas herramientas elegir una por encima de la otra, pues ambas operan en sistemas operativos distintos, lo que impide una comparación directa. No obstante, se puede afirmar que las dos herramientas son muy rápidas en la captura de datos, disponen de varias opciones de captura, distintos modos de ejecución, compresión y cálculo de hash de la evidencia, y son fáciles de utilizar. Además, tanto WinPMem como LiME son herramientas open source, disponibles en repositorios de Github abiertos al público, fáciles de obtener y de comprobar la seguridad del código descargado, sin licencias comerciales o disponibilidad limitada. Si el objetivo es adquirir la memoria volátil de un equipo, por ejemplo en una investigación forense de respuesta ante incidentes, estas dos herramientas cumplirán su trabajo de manera satisfactoria, superior a otras opciones disponibles, cubriendo los dos sistemas operativos más extendidos de la actualidad.

8. Conclusiones

La adquisición de memoria volátil de un equipo es una tarea fundamental en un proceso de análisis forense, siendo necesaria su obtención para poder examinar las posibles causas del incidente. Para agilizar el proceso de investigación, se hace necesaria la utilización de una herramienta que permita capturar los datos de la memoria de manera simple, rápida y eficaz. Es aquí donde cobran relevancia las herramientas de adquisición de memoria RAM. Además de las características mencionadas anteriormente, estas herramientas deben garantizar la integridad de la evidencia obtenida, para que pueda ser utilizada como prueba real.

En este análisis se ha realizado una comparación práctica y objetiva de varias de las herramientas de adquisición de memoria RAM más extendidas en la actualidad, en los sistemas operativos más relevantes actualmente, como son Windows 10 y Ubuntu 20.10. Para ello, se ha seguido un proceso bien definido de análisis de características principales y secundarias, dando una valoración numérica al final del análisis de cada herramienta. Se ha realizado una prueba práctica en la que se ha demostrado la velocidad de captura de cada herramienta en disco duro HDD y SSD, comparando el impacto en el rendimiento de la CPU, memoria y disco duro durante la propia captura. También se han indicado las características adicionales a la captura que presenta cada utilidad, siguiendo con otras características como la portabilidad, el tamaño total que ocupa en disco, el tipo de licencia que utiliza y la facilidad de uso de la herramienta. Una vez analizadas por separado, se han mostrado todas las características de las utilidades en una tabla comparativa, siguiendo con una clasificación según el mejor apartado de cada herramienta. Al final, se ha seleccionado una herramienta como la definitiva, que junta lo mejor de todas y que es la más indicada para un uso general de captura de datos de la memoria RAM.

En conclusión, tras realizar la comparativa, todas las herramientas aportan alguna característica distinta frente a otras, lo que hace escoger una herramienta por encima de otra especialmente complicado y subjetivo. En el fondo, la mejor herramienta será la más adecuada a la tarea que se esté desempeñando, y elegir una u otra dependerá de los gustos y conocimientos del usuario que la vaya a utilizar. En esta comparativa se han proporcionado categorías para la mayoría de casos posibles en los que se utilizaría una utilidad de este tipo, quedando la decisión final a elección del investigador o usuario final.

9. Trabajo futuro

El trabajo futuro consistirá en continuar con el análisis de otras herramientas de adquisición de memoria RAM, pues es posible que existan otras opciones interesantes en cuanto a obtención de memoria volátil en equipos informáticos. Un análisis similar al presentado en este trabajo, añadiendo alguna sección adicional puede resultar útil para investigadores forenses. También se puede ampliar el alcance de las herramientas a otros sistemas operativos o dispositivos, como el ejemplo de LiME y la captura en dispositivos móviles.

Siguiendo con el tema del análisis forense, el trabajo futuro puede continuar con la siguiente fase tras la captura de la memoria, el análisis de la evidencia. Se podría realizar una comparativa de herramientas de análisis de archivos de volcado de datos, otras que no sean la conocida Volatility. También se puede continuar con el análisis presentado pero centrándolo más en las características forenses, como por ejemplo comparando las capturas obtenidas en función de la integridad y si han modificado la memoria física del equipo durante la captura.

Por último, a partir de este trabajo se puede decidir la creación de una herramienta de adquisición de memoria RAM, tanto en Windows como en Linux. En este trabajo se han expuesto qué características son las más relevantes y necesarias que hacen que una herramienta destaque por encima de otra, por lo que ya se tienen las pautas iniciales sobre qué componentes básicos debería tener una posible utilidad similar a las analizadas.

10. Coste del proyecto

Realizar este proyecto ha tenido el siguiente coste en términos de personal.

Trabajo	Horas	Coste por hora (€/H)	Coste total
Investigación	115	25	2.875,00
Análisis	95	27	2.565,00
Redacción	70	20	1.400,00
Pruebas	20	23	460,00
Total	**300**	**-**	**7.300,00**

Tabla 4. Coste del personal del proyecto

El trabajo de investigación incluye todas las búsquedas realizadas en distintos papers, revistas de investigación, sitios web y documentación oficial de cada herramienta. El trabajo de análisis distingue la información útil y relevante de la insustancial, y asegura que los datos expuestos sean verídicos. La fase de redacción incluye todo el trabajo de elaboración de la memoria, incluyendo los textos escritos, la elaboración de tablas y colocación de capturas. Por último, el trabajo de pruebas consiste en todo el proceso desde la creación de los escenarios hasta las pruebas técnicas con cada herramienta.

A continuación se detallan los costes en hardware del proyecto.

Hardware	Coste (€)
Estación de trabajo	1.500,00
Teclado	100,00
Ratón	50,00
Monitor	200,00
Unidad usb	15,00
Total	**1.850,00**

Tabla 5. Coste hardware del proyecto

Los costes software del proyecto son los siguientes.

Software	Coste (€)
Windows 10	145,00
Microsoft Office 365	69,00
Oracle VirtualBox	0
Ubuntu 20.10	0
Herramientas de pruebas	0
Cronómetro de windows	0
Total	**214,00**

Tabla 6. Costes software del proyecto

En total, los costes del proyecto son los siguientes.

Tipo de coste	Coste
Personal	7.300,00
Hardware	1.850,00
Software	214,00
Total	**9.364,00**

Tabla 7. Costes totales del proyecto

El coste total del Proyecto, incluidos los gastos personales, de hardware y de software, asciende a una cifra de NUEVEMIL TRESCIENTOS SESENTA Y CUATRO EUROS.

11. Bibliografía

[1] «Random-access memory», *Wikipedia*. may 10, 2021. Accedido: may 10, 2021. [En línea]. Disponible en: https://en.wikipedia.org/w/index.php?title=Random-access_memory&oldid=1022460601

[2] «Understanding RAM and DRAM Computer Memory Types». https://www.atpinc.com/blog/computer-memory-types-dram-ram-module (accedido may 13, 2021).

[3] M. Mills, «DIMM vs SO-DIMM: Characteristics, Definition and Differences | ITIGIC», may 19, 2020. https://itigic.com/dimm-vs-so-dimm-characteristics-definition-and-differences/ (accedido may 16, 2021).

[4] «DDR3 vs DDR4 - Difference and Comparison | Diffen». https://www.diffen.com/difference/DDR3_vs_DDR4 (accedido may 16, 2021).

[5] «TEAMGROUP is Taking the Global Lead in the New DDR5 Generation-TEAMGROUP». https://www.teamgroupinc.com/en/news/ins.php?index_id=147 (accedido may 12, 2021).

[6] «About JEDEC | JEDEC». https://www.jedec.org/about-jedec (accedido may 12, 2021).

[7] «Corsair». https://www.corsair.com/uk/en/blog/ddr5-primer (accedido may 16, 2021).

[8] Z. A. Al-Sharif, H. Bagci, T. A. Zaitoun, y A. Asad, «Towards the Memory Forensics of MS Word Documents», en *Information Technology - New Generations*, Cham, 2018, pp. 179-185. doi: 10.1007/978-3-319-54978-1_25.

[9] «ISO/IEC 27037:2012», *ISO*. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/43/44381.html (accedido may 18, 2021).

[10] «rfc3227». https://datatracker.ietf.org/doc/html/rfc3227 (accedido may 18, 2021).

[11] thelma.allen@nist.gov, «CFTT Technical Information», *NIST*, may 09, 2017. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical (accedido may 18, 2021).

[12] P. I. Legal, «UNE 71506/2013. Metodología para el análisis forense de las evidencias electrónicas. • El Perito Informático», *El Perito Informático*, feb. 23, 2021. https://peritosinformaticos.es/une-71506-perito-informatico/ (accedido may 19, 2021).

[13] N. L. Petroni, Aa. Walters, T. Fraser, y W. A. Arbaugh, «FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory», *Digit. Investig.*, vol. 3, n.º 4, pp. 197-210, dic. 2006, doi: 10.1016/j.diin.2006.10.001.

[14] Timothy Vidas, «THE ACQUISITION AND ANALYSIS OF RANDOM ACCESS MEMORY». [En línea]. Disponible en: https://users.ece.cmu.edu/~tvidas/papers/JDFP06.pdf

[15] «FTK® Imager», *AccessData*. https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager (accedido jun. 08, 2021).
[16] F. Focus, «Evidence Acquisition Using Accessdata FTK Imager», *Forensic Focus*, mar. 02, 2018. https://www.forensicfocus.com/articles/evidence-acquisition-using-accessdata-ftk-imager/ (accedido jun. 12, 2021).
[17] «EFS - Encrypting File System - NTFS.com». http://ntfs.com/ntfs-encrypted.htm (accedido jun. 16, 2021).
[18] «PassMark OSForensics - Digital Investigation». https://www.osforensics.com/osforensics.html (accedido jun. 17, 2021).
[19] *Velocidex/WinPmem*. Velocidex, 2021. Accedido: jul. 04, 2021. [En línea]. Disponible en: https://github.com/Velocidex/WinPmem
[20] barrygolden, «MmMapIoSpace function (wdm.h) - Windows drivers». https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/wdm/nf-wdm-mmmapiospace (accedido jul. 07, 2021).
[21] Unknown, «Virtual Secure Mode and memory acquisition». http://blog.rekall-forensic.com/2018/09/virtual-secure-mode-and-memory.html (accedido jul. 07, 2021).
[22] «Belkasoft RAM Capturer: Volatile Memory Acquisition Tool». https://belkasoft.com/ram-capturer (accedido jul. 10, 2021).
[23] «Utilities | MoonSols». https://www.moonsols.com/resources.html (accedido jul. 12, 2021).
[24] «MAGNET RAM Capture», *Magnet Forensics*. https://www.magnetforensics.com/resources/magnet-ram-capture/ (accedido jul. 13, 2021).
[25] *504ensicsLabs/LiME*. 504ENSICS Labs, 2021. Accedido: jul. 14, 2021. [En línea]. Disponible en: https://github.com/504ensicsLabs/LiME
[26] «What is direct I/O anyway? - Alex on Linux». http://www.alexonlinux.com/what-is-direct-io-anyway (accedido jul. 14, 2021).
[27] «Ubuntu Manpage: memdump - memory dumper». http://manpages.ubuntu.com/manpages/trusty/man1/memdump.1.html (accedido jul. 14, 2021).